UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

Ingeniería en computación

Diagnóstico de la seguridad de información de UNICOMER-Nicaragua, en base al proceso DSS05 gestionar servicios de seguridad de COBIT 5.0

TRABAJO MONOGRÁFICO

Para optar al Título de

Ingeniero en Computación

Presentado por:

Br. Carlos José Ortiz Orozco **Carnet: 2009-30227**

Tutor:

Msc. Will Johnny Flores

Managua, Nicaragua

Marzo 2019

Dedicatoria

A Dios porque en su infinita misericordia nos brinda la vida, el tiempo y sabiduría para llegar este tiempo tan importante como es la presentación de este trabajo de culminación de estudios de grado.

A mi madre, mi abuela que con mucho esfuerzo me brindaron su apoyo en todo momento, por sus consejos, sus valores, por la motivación constante que ha permitido ser una persona de bien, ellas han sido clave para salir adelante en el proceso de mi formación académica.

Carlo José Ortiz

Agradecimientos

A Dios primeramente por permitirnos la elaboración de este trabajo monográfico y haberme dado salud y darme lo necesario para seguir adelante día a día para lograr mis objetivos.

A mi madre y abuela que han dado todo el esfuerzo para que yo ahora este culminando esta etapa de mi vida y darles las gracias por apoyarme en todos los momentos de mi vida.

Alvaro Zeledón, gerente de TI de la empresa UNICOMER, que en conjunto con su equipo nos brindaron su confianza y trasmitieron sus conocimientos y aportaciones que nos permitieron culminar este proyecto.

Al profesor Johnny Flores, que nos apoyó como tutor y con mucha paciencia nos daba sus orientaciones y compartía sus conocimientos y habernos llevado paso a paso para presentar este trabajo.

Gracias a todas las personas que apoyaron a la realización de este proyecto académico.

Carlos José Ortiz

Contenido

Lista de tablas

Lista de figuras

Lista de graficas

CAPITULO I:

INTRODUCCION

1. Introducción

Los gobiernos, las instituciones financieras, los hospitales y las organizaciones privadas tienen enormes cantidades de información confidencial sobre sus empleados, productos, investigación, clientes, etc. [1]. La información cada vez tiende a ser el activo más importante de las organizaciones, que, como cualquier otro activo importante, es necesario que esté protegida adecuadamente.

UNICOMER (Unión Comercial) es una organización compuesta de varias cadenas dedicadas a la comercialización de muebles, electrodomésticos, entre otros productos, con más 100 tiendas y presencia en todos los departamentos del país, sus oficinas centrales están ubicadas en Villa Progreso Rotonda La Virgen Costado Noreste.

UNICOMER tiene la necesidad de fortalecerse en temas de seguridad de la información por lo cual se realizará una evaluación de la gestión de la seguridad de información, ya que es un requisito del negocio por parte de un cliente y prácticamente se convierte en una obligación. La limitante para el desarrollo de la evaluación es que a solicitud de la empresa se omitirá el nombre del cliente y la reguladora de este.

Utilizando el proceso **DSS05 Gestionar Servicios de Seguridad**, de COBIT 5, se ejecutará una evaluación de seguridad de información, para identificar debilidades y fortalezas de seguridad en las TIC (tecnologías de la información y la comunicación) y así determinar el grado de madurez según COBIT 5.

1.2 Justificación

Para UNICOMER Nicaragua, es necesario reforzar los temas de seguridad de la información, ya que el negocio está creciendo y actualmente brinda servicios de TI e infraestructura (outsourcing) para un cliente que exige seguridad en su información, este cliente es regulado como se mencionó anteriormente en la introducción los nombres del cliente y su regulador no van a ser mencionado en el desarrollo del trabajo.

En correspondencia con lo anterior, la oficina gerencia de tecnologías de UNICOMER, expreso en una entrevista y en una carta que es beneficioso someterse a una evaluación de agentes externos a la organización, para identificar debilidades y medir el cumplimiento de las buenas prácticas o estándares de TIC y expone que de seguro el resultado del estudio será de apoyo para cumplir disposiciones generales que el cliente exige y será de utilidad para para nuestro proceso de mejora.

1.3 Objetivos

1.3.1 Objetivo General

Evaluar la seguridad de la información de UNICOMER-Nicaragua, empleando el proceso DSS05 gestionar servicio de seguridad de COBIT 5.0

1.3.2 Objetivos Específicos

1. Identificar los componentes del proceso gestionar servicios de seguridad de COBIT 5.0 en UNICOMER-Nicaragua

2. Determinar el grado de cumplimiento de la seguridad de información de UNICOMER-Nicaragua con respecto al proceso gestionar servicio de seguridad de COBIT 5.0

3. Determinar debilidades y fortalezas de la seguridad de información en UNICOMER-Nicaragua

4. Determinar el grado de madurez de la seguridad de información en base al modelo de madurez de COBIT 5.

CAPITULO II: MARCO TEORICO

2.1 COBIT

COBIT, en inglés: Control Objectives for Information and related Technology (Objetivos *de Control para Información y Tecnologías Relacionadas*). Es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenida por ISACA (en inglés: *Information Systems Audit and Control Association*) y el IT GI (en inglés: *IT Governance Institute*), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI.

2.2 COBIT 5

COBIT 5 es la última edición del framework mundialmente aceptado, el cual proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas. [3]

El modelo de referencia de procesos de COBIT 5 subdivide los procesos de gobierno y de gestión de TI de la empresa en dos principales áreas de actividad gobierno y gestión divididos en dominios de procesos:

- Gobierno: 1 dominio contiene 5 procesos.
- Gestión: 4 dominio contiene 32 procesos.

Esto proporciona un modelo de referencia de procesos que representa todos los procesos encontrados normalmente en una empresa respecto a las actividades de IT, ofreciendo un modelo de referencia común entendible para gerentes de operativa TI y de negocio. Cada empresa debe puede definir su propio conjunto de procesos, teniendo en cuenta su situación específica [11].

2.2.1 Proceso: Gestionar Servicios de Seguridad (DSS05).

Este proceso del área de gestión y del dominio *Entrega, Servicio y Soporte (DSS)* cubre los controles técnicos de seguridad para defender los recursos más críticos, vulnerables y sensibles incluyendo información (datos), infraestructura de redes y comunicaciones, puntos finales de red (por ejemplo, usuarios, PC) y acceso a sistemas. [2]

El proceso se divide en prácticas a su vez estas componen por actividades, son 7 prácticas y 49 actividades en el proceso DSS05.

Ejemplo:

Figura 1. DSS05 gestionar servicios de seguridad, Practica DSS05.01

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.01 Proteger contra software malicioso (*malware*). Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).	**De**	**Descripción**	**Descripción**	**A**
			Política de prevención de software malicioso	APO01.04
			Evaluaciones de amenazas potenciales	APO12.02 APO12.03
Actividades				
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.				
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).				
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.				
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).				
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).				
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.				

En la siguiente sección se presenta en detalles cada una de las prácticas de gestionar los servicios de seguridad de DSS05.

2.2.2 DSS05.01 Proteger contra software malicioso (malware).

El propósito de **DSS05.01** es implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso. [4]

Malware: Es la abreviatura de software malintencionado (del inglés "**mal**icious soft**ware**") y normalmente se usa para referirse a cualquier software diseñado para causar daño a una computadora, servidor o red informática. [5]

Actividades:

1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi automáticamente).
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.

2.2.3 DSS05.02 Gestionar la seguridad de la red y las conexiones.

Para ISACA, la seguridad de la red debe gestionarse activamente con una estrategia integrada y un conjunto de herramientas entre capas de red y topología. Por ejemplo, listas de control de acceso (ACL) en enrutadores y cortafuego (Firewall), Sistema de detección de intrusos (IDS). Los controles deben implementarse en todos los puntos de entrada, incluyendo correo electrónico, aplicaciones web, protocolos de transferencia de archivos, redes sociales, mensajería, puertos de aplicaciones / almacenamiento y hardware (USB). [2].

Actividades:

1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
4. Cifrar la información en tránsito de acuerdo con su clasificación.
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.
6. Configurar los equipamientos de red de forma segura.
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.

2.2.4 DSS05.03 Gestionar la seguridad de los puestos de usuario final.

Debe implementarse y administrarse la seguridad de punto final (software antivirus / antimalware, seguridad web / correo electrónico, cortafuegos) para asegurar que las computadoras portátiles, los equipos de sobremesa, los servidores y los dispositivos móviles estén adecuadamente protegidos (según el valor de la información) [2].

También se tiene que considerar la protección en contra las amenazas físicas y ambientales y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado. [7]

Actividades:

1. Configurar los sistemas operativos de forma segura.
2. Implementar mecanismos de bloqueo de los dispositivos.
3. Cifrar la información almacenada de acuerdo a su clasificación.
4. Gestionar el acceso y control remoto.
5. Gestionar la configuración de la red de forma segura.
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
7. Proteger la integridad del sistema.
8. Proveer de protección física a los dispositivos de usuario final.
9. Deshacerse de los dispositivos de usuario final de forma segura.

2.2.5 DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

La identidad del usuario y el acceso lógico deben ser gestionados en base a las necesidades del negocio y las bases menos privilegiadas.

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios **(creación, modificación y eliminación)**, a los sistemas y servicios de información. Prestar especial atención de los permisos de acceso con privilegiados, la asignación se debería restringir y controlar. [8]

Actividades:

1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
5. Segregar y gestionar cuentas de usuario privilegiadas.
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.

2.2.6 DSS05.05 Gestionar el acceso físico a los activos de TI.

Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias [2].

El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte [2].

Actividades:

1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.
3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.
5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y

disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.
7. Realizar regularmente formación de concienciación de seguridad física.

2.2.7 DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales de seguridad [2].

Documentos sensibles: Aquella información, así definida por su propietario, cuya revelación, alteración, pérdida o destrucción puede producir daños importantes a la organización propietaria de la misma [8].

Ejemplo de documentos sensibles: planes de negocio, proyectos, cuentas bancarias, cartera de clientes, código fuente de programa.

2.2.8 DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes [2].

Actividades:
1. Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.

3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.
4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

2.2.9 Las metas del proceso DSS05 son:

- La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.
- La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.
- Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.
- Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitido.
- La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida [3 del protocolo].

2.3 Evaluación de la capacidad y/o madurez de los procesos

COBIT 5 introduce una nueva forma de medir la madurez de los procesos a través del “Process Capability Model”, basado en el estándar internacionalmente reconocido “ISO/IEC 15504 Software Engineering – Process Assessment Standard” [9]. El proceso de evaluación supone determinar una calificación de capacidades para el proceso, lo que comprende:

2.3.1. Niveles de capacidades definidos (según ISO/ IEC 15504)

Tabla N˚1. Niveles de capacidad de procesos según ISO/IEC 15504

Niveles de capacidad	
Optimizado	El proceso es mejorado de forma continua
Predecible	El proceso establecido (Nivel 3) ahora se ejecuta dentro de unos límites definidos para alcanzar sus resultados.
Establecido	Implementado (Nivel 2) pero usando un proceso definido.
Gestionado	Esta implementado de forma gestionada (Planificado, Supervisado y Ajustado) y sus resultados son establecidos, controlados y mantenidos.
Ejecutado	Implementado alcanza su propósito.
Incompleto	No esta implementado o no alcanza su propósito.

2.3.2 Niveles de capacidad y atributos del proceso (ISO/IEC 15504-2)

Para evaluar el alcance de un nivel de capacidad determinado para un proceso, el estándar especifica una serie de atributos del proceso que están ligados a cada nivel de capacidad [10].

Tabla N˚2. Atributos genéricos de procesos para cada nivel de capacidad según ISO/IEC 15504-2

Escala	Atributos genéricos de procesos
Nivel 1	PA 1.1 Realización del proceso
Nivel 2	PA 2.1 Gestión del rendimiento del proceso PA 2.2 Gestión del resultado del trabajo
Nivel 3	PA 3.1. Definición del proceso PA 3.2. Despliegue del proceso
Nivel 4	PA 4.1 Medición del proceso PA 4.2. Control del proceso
Nivel 5	PA 5.1. Innovación del proceso PA 5.2. Optimización del proceso

2.3.3 Escala de calificación estándar (ISO / IEC 15504-2:2003)

Se requiere el establecimiento de una escala de calificación cuyos valores se basan en el porcentaje de logro de los atributos:

Tabla N°3. Escala de calificación según ISO/IEC 15504-2:2003

Niveles de calificación		
N	No Conseguido	0 a 15% de consecución
P	Parcialmente conseguido	>15% al 50% de consecución
L	Ampliamente conseguido	>50% al 85% de consecución
F	Totalmente conseguido	>85% al 100% de consecución

2.3.4 Indicadores sobre los cuales basar el logro de evaluación de cada atributo del proceso (sobre la base de ISO/IEC 15504-2:2003)

- **Nivel de capacidad 1**. Los indicadores son específicos de cada proceso y evalúan si se ha logrado el siguiente atributo: El proceso implementado logra su propósito. El nivel 1 se ocupa del contenido detallado de los procesos de COBIT 5, por lo que se debe definir el trabajo según los términos de COBIT 5.
- **Niveles de capacidad 2 a 5**. La evaluación de la capacidad se basa en indicadores de desempeño de procesos genéricos. Estos se denominan genéricos porque se aplican en todos los procesos, pero difieren de un nivel de capacidad a otro [10].

CAPITULO III: DISEÑO METODOLOGICO

3.1 Preparación para el estudio

De las actividades de cada práctica de gestión se formularon preguntas, un cuestionario por cada práctica.

Ejemplo:

Práctica DSS05.1 Actividad 2:

Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi automática).

Preguntas formulas a partir de la actividad 2 de DSS05.1

A. ¿Qué herramientas son activadas para proteger en contra de software malicioso?
B. ¿Cómo se actualiza el software antivirus y las definiciones de software malintencionados (Automática o Semiautomática)?

En este ejemplo debido a que la actividad es extensa, se formularon 2 preguntas, para un mejor entendimiento de las personas que van a responder estas preguntas.

De esta misma manera se formularon las preguntas de todas las actividades, en su mayoría una pregunta por actividad.

Son 7 cuestionarios, ver cuestionarios elaborados en Anexo 1.

3.1.1 Herramienta de apoyo.

Se elaboró plantilla en Microsoft Excel como herramienta de apoyo para el registro, procesamiento y presentación de resultados de manera ordenada, una pestaña diferente para cada práctica de gestión.

(Ver archivo en CD: “plantilla DSS05 vacía”)

3.1.2 Estructura de la herramienta de apoyo

A continuación, la estructura de plantilla en Microsoft Excel que consta de 15 pestañas:

- **Indicaciones:** Presenta todas las indicaciones para facilitar el uso de la plantilla y entendimiento de cada pestaña.
- **ModeloEvaluacion:** Resumen de la teoría necesaria para la evaluación de los procesos de COBIT5 con la ISO 15504-2:2003
- **DSS05:** Todo el contenido del proceso DSS05 Gestionar Servicios de seguridad de COBIT5 (Practicas, descripción y actividades)
- **EjemploUso:** Muestra cómo se debe completar cada pestaña, correspondiente a cada práctica de gestión.
- Las hojas "**DSS05.1** al **DSS05.7** obedecen al orden de las 7 practicas del proceso y contienen las preguntas, los campo para síntesis de repuestas y documentos, evidencias y calificaciones de las actividades de cada práctica.
- **Componentes:** Para presentar resumen de las actividades que se cumplen y de las que no se cumplen.
- **Indicadores:** Una tabla con los niveles de capacidad y los 9 atributos de procesos con sus respectivos objetivos genéricos.
- **EvaluaciónFinal:** Para presenta un resumen de la evaluación total del proceso.
- **DyF:** Para las Debilidades y Fortalezas según la evaluación del proceso.

3.2 Recopilación de la información

Para contestar los 7 cuestionarios elaborados, se sugiere la realización de entrevistas, y la solicitud de los respectivos documentos para recopilar la información.

3.3 Procesamiento de la Información

En base a las respuestas obtenidas para cada pregunta y la documentación proporcionada se realizará una síntesis de las repuestas y de información contenida en los documentos.
También se plantea la solicitud de evidencias y de ser posible realizar verificaciones de las declaraciones que se brindaron en las entrevistas, para realizar los comentarios necesarios de cada actividad y esto será de utilidad para pasar a la evaluación.

3.4 Evaluación

De acuerdo a la síntesis de las repuestas, la documentación, evidencias y verificaciones obtenidas, se dará una calificación en escala porcentual de 0 a 100, que representará el grado de cumplimiento de la actividad, para los casos que la actividad tenga 2 preguntas dividir el 100% del total de la actividad entre las 2 preguntas, de la misma manera se hará para cada actividad.

Una vez que se califiquen todas las actividades de cada práctica de gestión promediando las calificaciones obtendremos el grado de cumplimiento de la práctica de gestión que se esté evaluando (según el estándar ISO/IEC 15504-2:2033), luego el promedio de las calificaciones de las 7 prácticas obtendremos la calificación del proceso.

CAPITULO IV: ANALISIS Y RESULTADOS

4.1 Generalidades de la empresa

UNICOMER Nicaragua fue fundado en el año 2000 y sus operaciones comprenden de varias cadenas dedicadas a la venta al por menor de pequeños enseres, muebles, audio, video, productos electrónicos, accesorios y productos de óptica, motos, y una variedad de accesorios tecnológicos, con más de 100 tiendas a nivel nacional.

4.1.2 Misión de la empresa

Ser el líder en la comercialización de muebles, electrodomésticos, electrónicos y otros productos en los mercados que operamos, sirviendo las necesidades de nuestros clientes con productos y servicios financieros innovadores, con la dedicación y esmero que merecen, fomentando un ambiente profesional para el desarrollo de nuestros colaboradores y proveedores, sirviendo a nuestras comunidades y logrando un crecimiento sostenible para cumplir las expectativas de los accionistas.

4.1.3 Visión de la empresa

Ser una organización comercial y de servicios financieros de clase mundial que logra sus metas de negocio y responsabilidad social a través de un liderazgo ejemplar en un ambiente profesional diverso que promueva integridad, honestidad y respeto a los demás.

4.1.4 Ubicación

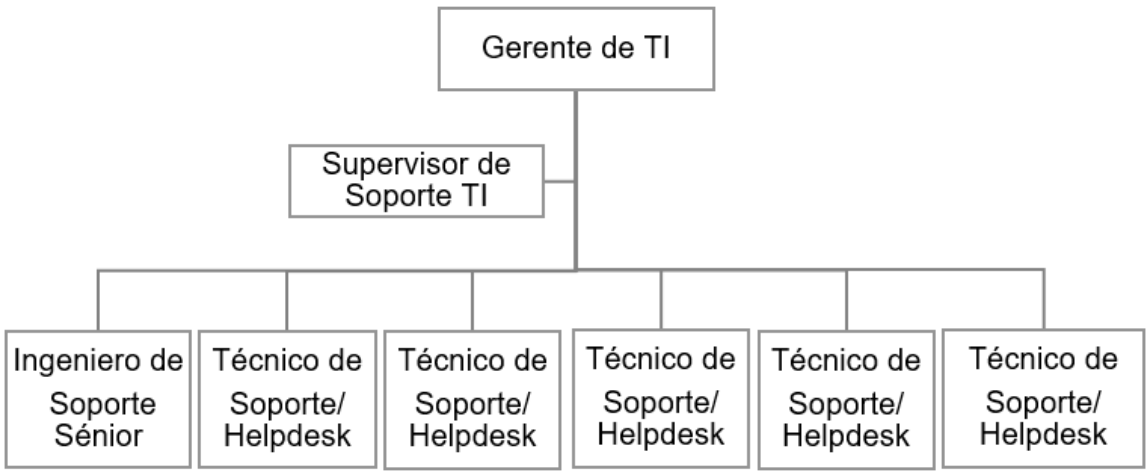
Las Oficinas Centrales se encuentran en costado noroeste de la rotonda La Virgen.

4.1.5 Área de TI

El área de TI está compuesta de 8 personas

1. Gerente de TI
2. Supervisor de soporte técnico
3. 1 Ingeniero de soporte sénior
4. 5 técnicos de soporte/Helpdesk

Figura 2. Organigrama Gerencia de Informática - UNICOMER NIC**.**



4.2 Conducción del estudio en UNICOMER

4.2.1 Presentación del instrumento a la gerencia de TI

Mediante una reunión con la oficina de gerencia de TI de UNICOMER Nicaragua, se propone el desarrollo de este estudio, se presentan los objetivos, el diseño metodológico y los instrumentos para diagnosticar la seguridad de la información.
La gerencia acepta y se procede a agendar otra entrevista para empezar a completar con los cuestionarios.

4.2.2 Agendar las entrevistas.

La gerencia de TI, era la encargada de contestar los 7 cuestionarios, pero con el fin de recopilar más información y hacer un diagnóstico objetivo, se solicitó entrevistar a una persona más del equipo de TI, las cual sus funciones estuvieran en correspondencia con el cuestionario a contestar.

4.2.3 Desarrollo de las entrevistas

Antes de empezar con el cuestionario, se exponía el nombre de la práctica, propósito de la práctica de gestión, para ubicar en contexto al entrevistado, se leía textual cada actividad antes de realizar las preguntas correspondientes.
Se realizaron 4 entrevistas con la oficina de gerencia de TI para completar los 7 cuestionarios, según su agenda y tiempo disponible.

En las mismas fechas y para contestar los mismos cuestionarios se entrevistó a las otras personas del equipo de TI.
A continuación, presentamos un resumen de las entrevistas realizadas.

Tabla N°4. Entrevistas realizadas para completar Cuestionarios.

Cuestionario	Fecha	Cargos de los responsables de responder los cuestionarios	Áreas
C1	22/11/17	Gerente de TI, Técnico de Soporte y Asistente de la gerencia de RRHH	TI y RRHH
C2	22/11/17	Gerente de TI y Técnico de Soporte	TI
C3	11/12/17	Gerente de TI y Técnico de Soporte	TI
C4	11/12/17	Gerente de TI, Ingeniero de soporte sénior	TI
C5	13/12/17	Gerente de TI, supervisor de soporte técnico, Arq. Encargada de proyectos	TI y proyectos
C6	18/12/17	Gerente de TI y supervisor de soporte técnico.	TI
C7	18/12/17	Gerente de TI y supervisor de soporte técnico.	TI

De acuerdo con las repuestas brindadas en la pregunta 1 del cuestionario C1, se tuvo la oportunidad de entrevistar a la responsable del área de RRHH, quien es la encargada de enviar las comunicaciones masivas por correo.

De la misma manera en la pregunta 5 del cuestionario C5, se tuvo la oportunidad de entrevistar al responsable del área de proyectos, encargada del control del acceso.

Ver Anexo 2 para ver los cuestionarios completados.

4.2.4 Solicitud de evidencias y verificaciones

Luego de completar los cuestionarios, de acuerdo a las declaraciones dadas, se solicitaron evidencias, en algunos casos solicitamos visitas en sitio para realizar verificaciones.

Ejemplo:

- Verificación de actualización diaria del Antivirus
- Verificación de la existencia de un Firewall

Ver anexo 3 y ver todas las verificaciones en archivo en CD: “plantilla DSS05” o carpeta Evidencias

4.2.5 Uso de las pestañas de plantilla DSS05

Ejemplo pestaña “*DSS05.01”* (Proteger contra software malicioso)

Actividad 1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.

Figura 3. Extracto de la pestaña *DSS05.3*

A	B	C	D	E	F
DSS05.03 Gestionar la seguridad de los puestos de usuario					
Detalles de las Actividades					
Actividad	**Pregunta**	**Sintesis de las entrevistas y referencia de documentos**	**Comentarios**	**Calificación**	**Evidencia**
1. Configurar los sistemas operativos de forma segura.	¿Qué actividades realizan hacer más seguros los sistemas operativos y reducir las vulnerabilidades?	• Se desinstalan aplicaciones innecesarias • Uso de Antivirus • Los usuarios no tiene permiso de administrador sobre el sistema operativo. • Bloque de puertos USB • Se enrolan al dominio, y se aplican politicas de grupos (GPO) • Política de Seguridad en los equipos tecnologicos (Política de la seguridad de la información, #15)	Se cumple, según muestra de equipos revisado para la validación de las respuesta.	**100%**	Actividades para fortalecer los sistemas operativos
2. Implementar mecanismos de bloqueo de los dispositivos.	¿Cuáles son los mecanismos de bloqueo que se implementan en los dispositivos del usuario final?	• Las portatiles se le colocan contraseña de arranque (BIOS) y de disco duro. • Bloqueo el usuarios luego de varios(3,4,5) intentos fallidos, tanto en los sistemas de información y el sistema operativo. • Bloqueo de sesion por inactividad luego de 5 minutos. • Bloqueo de acceso a memorias USB	Se cumple, según muestra de equipos revisado para la validación de las respuesta.	**100%**	Mecanismo de bloqueo dispositivos de usuario.
3. Cifrar la información almacenada de acuerdo a su clasificación.	¿Se cifra la información almacenada en los dispositivos, de acuerdo con su clasificación ?	A los disco duros externos se cifran con BitLocker y los discos duros de portatil se colocan contraseña desde el BIOS. Se aseguro en la entrevista que: *por lo general los usuarios de portátil son los usuarios que manejan información importante* .	No está documentado que los usuarios de portátil son los que manejan información crítica o importante.Para más detalles de la clasificación de la información de la organización. Revisar Actividad 4	**30%**	Disco Bloqueados y Cifrados

Pestañas para la evaluación de cada práctica.

- En la parte superior hace referencia a la práctica de gestión que se trabajara.
- La columna **A** hace referencia al número de la actividad.
- La columna **B** se presentas las preguntas formuladas para su correspondiente actividad.
- La columna **C** es para detallar una síntesis de las respuestas obtenidas en las entrevistas y en caso de hacer referencia de documentos. (Al final de la columna vincular la entrevista)
- La columna **D** Se escriben los comentarios acerca de las declaraciones de los entrevistados, las evidencias y verificaciones correspondientes a la pregunta.

- La columna **E** Se establece una calificación en escala porcentual, según los resultados de la actividad, al final de la columna se plasma la calificación total de la práctica y a la par colocar la escala de calificación según la ISO/IEC 15504-:2003 (N, P, L, F).

  Para los casos que la actividad tenga 2 preguntas, se dividirá en 50% para pregunta.
- La columna **F** columna para vincular las evidencias obtenidas.

En la siguiente sección se presenta:

4.3 Como se completó la plantilla DSS05. Cada una de las prácticas de gestión con la información registrada, procesada y las calificaciones de las prácticas.

Tabla N°5. Procesamiento de información en la plantilla DSS05 de práctica DSS05.1

DSS05.01 Proteger contra software malicioso (malware).

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencias
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	¿Cómo se concientiza sobre software malicioso?	Se envía botines informativos a través de correo a los diferentes grupos de distribución (a nivel de servidor de correo) desde una cuenta llamada *Comunicación Interna NIC.*	Se logra verificar los comunicados enviados por parte de Capital Humano(RRHH) (Se entrevisto a la encargada de enviar las Comunicaciones Internas),a los diferentes grupos de distribución.	**50%**	Ultimos Boletines Informativos
	¿Cómo se refuerza los procedimientos preventivos y responsabilidades sobre software malicioso?	Los equipos(Computadoras), se preparan por parte de TI con todo el software de protección y luego se realiza entrega formal al usuario y pasa a ser el responsable del equipo. Según el documento **Política de Seguridad de Información:** En **#15.1.2** Se declara: *Soporte IT deberá cerciorarse de que todos los equipos deben ingresarse al dominio, con sistema operativo actualizado, con todos los parches de seguridad remendados y liberados a la fecha, con SCCM , Antivirus y con todo el software de seguridad requerido y actualizado.* En **#14** Los colaboradores son responsables de la creación y administración de respaldos de la información electrónica contenida en sus equipos.	No hay procedimiento explicito, para la prevención de software malicioso. Según la *Política de seguridad de la información* Soporte IT es responsable de que todos los equipos tengan todo el software de seguridad instalado y actualizado. Por otra parte, también vemos que se indica que el usuario también se tiene que hacerse responsable de su información.	**10%**	
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi automáticamente).	¿Qué herramientas son activadas para proteger en contra de software malicioso?	De acuerdo a la entrevista realizada al gerente de TI y el tecnico se activan: Antivirus McAfee VirusScan Enterprise + AntiSpyware Enterprise+McAfee DLP Endpoint . Herramientas de respaldo automático para usuarios claves.	Se verifico que utilizan McAfee Agent 5.3.y McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8.	**50%**	Verificación del uso de antivirus ,de una muestra de 10 equipos de usuarios.
	¿Cómo se actualiza el software antivirus y las definiciones de software malintencionados (Automática o Semiautomática) ?	Las actualizaciones son automáticas, todos los equipos desde su entrega van con un agente de McAfee y este se gestiona las actualizaciones que se localizan en un servidor.	Se actualiza diario, automáticamente a través del agente.	**50%**	
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	¿Cómo distribuyen todo el software de protección? ¿Es centralizado?	Cuentan con una herramienta llamada System Center Configuration Manager (SCCM) y OCS Inventory para distribuir software de forma centralizada.	Se distribuye el software de protección de forma centralizada a través de la consola de **ePolicy Orchestrator (ePO)**, para actualizar el agente se realiza despliegue por SCCM y OCS Inventory.	**50%**	Verificación de la gestión de cambios y las configuraciones desde la consola de McAfee
	¿Cómo se gestiona el cambio y configuración de software de protección?	Todos las configuraciones y cambios se realizan en el servidor por medio de la consola de McAfee ePolicy Orchestrator (McAfee ePO)	Se logra verificar la centralización de la gestión de configuraciones y cambios desde la **ePO**	**50%**	
4.Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	¿Cómo se revisa y evalúa periódicamente la información sobre nuevas potenciales amenazas de malware? (Ejemplos: Revisando productos de proveedores y servicios de alertas de seguridad)	Existe un comité de seguridad conformado por miembros de diferentes países de la región de Centroamérica entre ellos el gerente de TI, Nicaragua y dos veces al mes se comunican en conferencia para ver temas relacionados a la seguridad de TI. (Respaldos, Antivirus, usuarios administradores, Nuevas amenazas. etc.).	Se logra evidenciar el trabajo del comité de seguridad y efectivamente estan pendiente de las nuevas amenzas que reportan los proveedores.	**100%**	Evaluaciones de nuevas potenciales amenazas
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	¿Cómo se filtra el tráfico entrante de internet , para evitar correos de phishing y descargas de software espías ?	El tráfico se filtra mediante el Firewall, McAfee analiza la recepción de correos electrónicos y también de programas no deseados.	Se logro evidenciar la integracion de un complemento de McAfee con el cliente de correo electronico MS Outlook.	**100%**	Integración del cliente de correo Outlook con McAfee
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	¿Cómo educan y capacitan a los usuarios respecto al tema de malware en el correo electrónico, el uso del internet y el no instalar software no autorizadas?	Se imparten charlas en la induccion del personal de nuevo ingreso con los temas: • Seguridad de la información • Correo Electronico • Uso del Internet • Instalar Software No Autorizado Se refuerza con recordatorios por correo electronico a los diferentes grupos de distribución.	Estas charlas son solomente para los de nuevo ingreso. También no se detalla en las diapositivas el tema de malware.	**5%**	Temas y la asistencia de las charlas impartidas
		Entrevista DSS05.01	**Calificación de la practica DSS05.1:**	**77%**	**L**

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	**P-** >15%-50%	**L-** >50%-85%	**F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Tabla N°6. Procesamiento de información en la plantilla DSS05 de práctica DSS05.2

DSS05.02 Gestionar la seguridad de la red y las conexiones.

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencias
1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	¿En función de las evaluaciones de riesgos y los requisitos del negocio, cuentan con una politica de seguridad de las conexiones?	Existe una politica general de nivel de la región "*Politica de seguridad de la información*", esta contiene una seccion de: • Uso de correo electronico •Acceso a Internet, Redes Sociales y Mensajeria Instantanea •Trabajo Remoto/Acceso VPN y redes inalambricas. Estan politica esta alineada a los requisitos del negocio a nivel de la region(C.A) pero no cuentan con una evaluacion de riesgos, indican que se encuentran trabajando en los riesgos del negocio, para alinear aun más la politica al pais.	No cuenta con evaluacion de riesgos,(esta en proceso) por lo tanto la politica no esta alineada a una evaluación de riesgo, esta ajustada a los requerimientos del negocio a nivel de la región (C.A)	**10%**	Politicas de las conexiones
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	¿Cómo se garantiza y controla que solo los dispositivos autorizados tengan acceso a la información y a la red empresarial?	Todos los sistemas de información solicitan usuario y contraseña para el ingreso, incluyendo el sistema operativo. Para el acceso a la red, inalámbrica se necesita usuario y contraseña, para el acceso a la red mediante cable no hay restricción , cualquier equipo se puede conectar.	El ingreso a los sistemas de información en red se controla mediante el uso usuario y contraseña, diferentes roles,perfiles. Los puntos de acceso a la red mendiante cablea no cuenta con ninguna restricción, para conectarse a la red.	**35%**	Dispositivos autorizados con acceso a la información y red de la empresa y forzados a solicitar contraseña.
	¿Se configura estos dispositivos para que solicite contraseña?	SI, Uso de credenciales de acceso.	Todo los dispositivos solicitan usuario y contraseña.Incluyendo para ingresar a la configuraciones de los equipos.	**50%**	
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	¿Con qué mecanismos de filtrado de red cuentan (Firewall, Software de detección de intrusos?	Existe un Firewalls Cisco ASA y Servidor proxy , para filtrar trafico de los usuarios a internet.	En el centro de datos se valido la existencia de un Firewall Cisco ASA 5520. Se verifico el uso de proxy para filtrar el contenido del internet para los usuarios.	**50%**	Mecanismos de filtrado de red.
	En estos mecanismos ¿cuáles son las políticas de control de acceso configuradas que se consideran más importantes para el filtrado de tráfico entrante y saliente?	•El permitir las redes de la empresa y las conocidas (seguras). •Bloquear los puertos de conexión y permitir solo los aprobados o seguros. •Para lo de salida esta el proxy para que los usuarios no tenga acceso total a internet.	No se logro verificar las reglas en el firewall, no logramos la entrevista con el administrador del mismo, ya que no es parte equipo de TI de Nicaragua.	**50%**	
4. Cifrar la información en tránsito de acuerdo con su clasificación.	¿La información en tránsito está encriptada de acuerdo con su clasificación?	No esta encriptada. Según el documento *Politica de Seguridad de la informacion* #7: *Por defecto , toda información que se maneje dentro de la compañia será clasificada como "confidencial"*	No hay metodo o herramienta que pueda clasificar la información en transito. No se tiene herramienta o metodo para cifrar la información en transito.	**0%**	Guías de Clasificación de la información.
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.	¿A nivel de conectividad que protocolos de seguridad se utilizan?	Se utiliza HTTPS, SSH , VPN (IP SEC), SSL, Telnet.	Se validó el uso de los protocolocos dictados en la entrevista. Algunos equipos aún tiene activado el protocolo Telnet, protocolo con problemas de seguridad.	**90%**	Protocolos usados para las conexiones de red.
6. Configurar los equipamientos de red de forma segura.	¿Se configuran los equipos de red de forma segura?	Si	Todos los equipos tomados como muestra están configurados con credenciales de acceso, límite de tiempo sin actividad.	**50%**	Parametros de seguridad en los equipos de red.
	¿Cuáles son los parametros de seguridad configurados en los equipos activos de red (Enrutadores,Conmutadores,Puntos de acceso)?	• Usuario y contraseña • Desconectar la sesión luego de 30 segundos sin actividad. • Habilitar la conexión mediante SSH y HTTPS • 3 intentos de contraseña incorrecta y se cierra la conexión	Protocoló de conexión SSH, HTTPS, HTTP y Telnet, este último es considerado un protocolo inseguro y se encontró configurado en algunos equipos viejos que no aceptan conexión SSH.	**40%**	
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	¿Qué mecanismos de confianza se establecen para dar soporte a la transmisión y recepción segura de la información?	• Proxy (Filtrado WEB) • Protocolos Seguros (VPN, SSH, HTTPS) • Firewall • Antivirus (McAfee Enterprise) • Politicas de grupo en Active Directory	Se verifico la implementación de: • Filtrado web, • Firewall, • Herrmamientas antivirus, • protocolos de conexión segura a excepción de telnet. Sin embargo un mecanismo de confianza importante en la transmision y recepción segura de la información es que esta vaya encriptada.	**85%**	• Proxy (Filtrado WEB) y Firewall, Ver **Actividad 3** • Protocolos Seguros (VPN, SSH, HTTPS), Ver **Actividad 5** • Antivirus (McAfee Enterprise), **Ver practica DSS05.01**
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	¿Realizan pruebas de intrusión ("Ethical Hacking") para determinar el nivel de proteccion de la red? ¿Con que frecuencia?	No	Esta actividad no se cumple.	**0%**	**N.A**
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	¿Realizan pruebas periódicas para determinar la adecuación de la proteccion de los sistemas de información?	No	Esta actividad no se cumple.	**0%**	**N.A**
		Entrevista DSS05.2	**Calificación de la practica DSS05.2:**	**51%**	**L**

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	**P-** >15%-50%	**L-** >50%-85%	**F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Tabla N°7. Procesamiento de información en la plantilla DSS05 de práctica DSS05.3

DSS05.03 Gestionar la seguridad de los puestos de

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencia
1. Configurar los sistemas operativos de forma segura.	¿Qué actividades realizan hacer más seguros los sistemas operativos y reducir las vulnerabilidades?	• Se desinstalan aplicaciones innecesarias • Uso de Antivirus • Los usuarios no tiene permiso de administrador sobre el sistema operativo. • Bloque de puertos USB • Se enrolan al dominio, y se aplican politicas de grupos (GPO) • Política de Seguridad en los equipos tecnologicos (Política de la seguridad de la información, **#15**)	Se cumple, según muestra de equipos revisado para la validación de las respuesta.	**100%**	Actividades para fortalecer los sistemas operativos
2. Implementar mecanismos de bloqueo de los dispositivos.	¿Cuáles son los mecanismos de bloqueo que se implementan en los dispositivos del usuario final?	• Las portatiles se le colocan contraseña de arranque (BIOS) y de disco duro. • Bloqueo el usuarios luego de varios(3,4,5) intentos fallidos, tanto en los sistemas de información y el sistema operativo. • Bloqueo de sesion por inactividad luego de 5 minutos. • Bloqueo de acceso a memorias USB	Se cumple, según muestra de equipos revisado para la validación de las respuesta.	**100%**	Mecanismo de bloqueo dispositivos de usuario.
3. Cifrar la información almacenada de acuerdo a su clasificación.	¿Se cifra la información almacenada en los dispositivos, de acuerdo con su clasificación ?	A los disco duros externos se cifran con BitLocker y los discos duros de portatil se colocan contraseña desde el BIOS. Se aseguro en la entrevista que: *por lo general los usuarios de portátil, son los usuarios que manejan información importante* .	No está documentado que los usuarios de portátil son los que manejan información cítrica o importante.Para más detalles de la clasificación de la información de la organización. Revisar *Actividad 4 de DSS05.02.*	**30%**	Disco Bloqueados y Cifrados
4. Gestionar el acceso y control remoto.	¿Cómo se gestiona el acceso remoto y control de los equipos de usuario final?	Los equipos ya van preparados con la aplicación llamada VNC server y cuando el usuario necesita apoyo se solicita la direccion IP del equipo y asi se tiene control total del este.	Se realizarón las pruebas de conexión remota a equipos de usuarios.	**100%**	Gestión de acceso remoto y control de los equipos
5. Gestionar la configuración de la red de forma segura.	¿Cómo administran la configuración de red de forma segura en los dispositivos de los usuarios ?	Todas las computadora pueden acceder a la red e intranet conectandose a traves de los puntos de red y la configuración del equipo se realiza automaticamente(Mediante el servicio DHCP). Pero para el accesos a internet existen perfiles de navegacion establecidos (grupos de paginas web) de acuerdo al rol del colaborador. Para el acceso a la red inalambrica se tiene que agregar la red manualmente(colocar el nombre de la red, tipo de seguridad y autenticación) y luego solicita usuario y contraseña. En la **Politica de acceso a los sistema o aplicativos informaticos, #6.9** se plantea las reglas de : *Acceso a Internet,redes sociales y mensajeria instantánea.*	Por medio de cable de red, cualquier equipo tiene acceso a la red y no tienen acceso a internet. Por la conexión inalámbrica (solo portátiles), tienen acceso libre a internet. No se cumple con lo declara la *Política de acceso* en el **#6.9**, ya que todos los usuarios de portátil mediante la red inalámbrica tienen acceso full a internet	**60%**	Verificación de configuración segura de la redes
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	¿Se implementa el filtrado del tráfico de red, en dispositivos de usuario final? ¿Como?	Si, mediante proxy . Para los usuarios de portatil con accceso a red inalambrica tienen acceso sin restricciones a internet.	Los usuarios de red inalámbrico no se les aplica filtro de red, según repuesta de técnico. Revisar Actividad 3 de DSS05.2 Mecanismos de filtrado de red	**85%**	**Revisar DSS05.2, Actividad 3**
7. Proteger la integridad del sistema.	¿Cómo protegen la integridad de los sistemas operativos?	• Los usuarios no tienen permiso de administrador, para que no realicen cambios en el sistema operativo y no instalen programas. • Bloqueo de USB • Uso de Antivirus actualizado • Uso de estabilizador electrico (UPS)	Se validan repuestas con muestra de equipos de usuarios.	**100%**	• **Actividad 1,2 y 8** • **Practica DSS05.1**
8. Proveer de protección física a los dispositivos de usuario final.	¿Cuáles son las medidas de protección a nivel físico con la que cuentan los dispositivos de usuario final?	• Puntos electricos protegido por UPS. • Se brinda un cable de seguridad a los usuarios de equipos portatiles. • Ubicación libre de amenzas ambientales • Guardias de seguridad fuera de las oficinas • Se transfiere la responsanbilidad de los dispositivos • Politica de Seguridad en los equipos tecnologicos (Politica de la seguridad de la información, **#15**)	Se validó todas medidas. No se encontró evidencia de ejecución de un plan de mantenimiento preventivo para los equipos (se considera una medida de protección física muy importante).	**85%**	Medidas de Protección a nivel fisico
9. Deshacerse de los dispositivos de usuario final de forma segura.	¿Cuál es el procedimiento para desechar los dispositivos de usuario final de forma segura?	Las repuestas de los entrevistados: 1. Esta descrito en la **Politicas para Administracion Fisica y logica de los dispositivos** (**#4.19** Desecho de equipos). 2. Se verifica que no tenga valor en libros con Contabilidad, pasa a la bodega y luego se desechan, para esto se levanta un acta del descarte, junto con el responsable de activo fijo de contabilidad, se retiran los discos duros, si es para desecho y si es venta o donación se formatean.	Se logra verificar el procedimiento para deshacerse de los equipos de usuarios final, planteada en la Politicas para *Administracion Fisica y logica de los dispositivos* (#4.19 Desecho de equipos). Ver evidencia.	**100%**	Desechar dispositivos de forma segura
		Entrevista DSS05.3	**Calificación de la practica DSS05.3:**	**84%**	**L**

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	**P-** >15%-50%	**L-** >50%-85%	**F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Tabla N°8. Procesamiento de información en la plantilla DSS05 de práctica DSS05.4

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencias
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	¿Los accesos otorgados a cada usuario en los diferentes aplicativos son de acuerdo con el rol y la función definidos para la unidad de negocio correspondiente?	Si hay diferentes perfiles o roles de acuerdo con las funciones que desempeñen.	Se verificaron los roles y el funcionamiento de estos en los sistemas.	50%	Roles en aplicativos
	¿Se alinea la asignación de roles, funciones y responsabilidades definidas en los sistemas, basándose en los principios de menor privilegio?	Si , Se alinea, siempre que se define cada módulo capaz de acceder solo a la información y recursos necesario para su legítimo propósito, limitando a la menor cantidad de privilegios para desarrollar acciones.	Se encontraron roles con los mínimos accesos, menús limitados, roles solo de consulta.	50%	
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.	¿Se identifica de manera única todas las actividades de procesamiento de información por roles?	Si, previamente se recaba la información requerida para cada rol.	se logró verificar roles con el detalle de funciones, actividades o menús asignados.	50%	Actividades por roles y coordinación con el negocio
	¿Coordinan los roles con las unidades del negocio y aseguran que todos los roles están definidos consistentemente, incluyendo los roles definidos por el propio negocio?	Si, se involucran a todas las unidades de negocios al generar los perfiles para cada rol en dependencia de las necesidades.	Según la política de acceso a los sistemas informáticos, la creación de nuevos roles o menús, tiene que estar basado en una necesidad del negocio y el usuario propietario de la aplicación se encarga de hacer un análisis para evitar crear roles innecesarios.	50%	
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	Basandose en su clasificacion de seguridad ¿Se autentica todo acceso a los activos de información y asegurando que los controles de autenticación han sido administrados adecuadamente?	Si, cada acceso tiene permisos limitados de acciones dependiendo del rol. En la fase de control de calidad de aplicaciones se realizan muchos escenarios antes de que la aplicación salga a producción. Se generan niveles de seguridad a partir de la administración de la base de datos, además de activar los logs y triggers y bitácoras donde se reflejen los cambios.	Se autentica el acceso a los activos de información, mediante usuario y contraseña para aplicación o sistema, pero no está basado en una clasificación de seguridad.	15%	Autenticación de acceso a los activos de información
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	¿Como se manejan las altas, bajas y cambios de accesos en los sistemas de información?	Solicitudes escritas con su respectivo formato y autorización del jefe de área.	Existen una politica de acceso a los sistemas y un procedimiento para el proceso de altas,bajas y cambios en los sistemas de información.	50%	Altas,Bajas y cambios de accesos a los sistemas
	Esta gestión de acceso ¿Son las transacciones aprobadas, documentadas y autorizadas?	Si	Se verificaron que las transacciones son aprobadas , documentadas y autorizadas.	50%	
5. Segregar y gestionar cuentas de usuario privilegiadas.	¿Como se gestionan y separan los niveles de acceso privilegiado?	Ambos entrevistados concuerda: Que sé tiene que justificar los accesos el acceso priviligeado y tiene se autorizados por el usuario propietario de la aplicación. Según documento **Politica de accesos a los sistemas Informaticos #10.2:** *Los accesos privilegiados,súper-usuarios o usurios tecnicos, deben ser autorizados por el usuario propietario del aplicativo, y,secundado por ele Gerente Corporativo de Servicios y Operaciones de IT (o el gerente de IT en el caso de aplicaciones de pais, no corporativas),usando los procedimientos y formatos vigentes descritos en esta politica.*	Esta establecido el procedimiento para controlar el acceso de los usuarios con acceso privilegiado a los sistemas de información. (Más detalle en las evidencias.) En la evidencia se encuentra las definiciones de usuarios según la organización.	100%	Gestión de usuarios privilegiados
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	¿Realizan revisiones periódicas de la gestión de todas las cuentas y niveles de privilegios relacionados?	Si, se generan reportes de usuarios y el usuario propietario es quien debe llevar el control de las cuentas de usuario con privilegio.	Según la *Politica de accesos a los sistemas informaticos* , Los especialistas de soporte de aplicaciones generan reportes periodicamente y los envia al usuario propietario de la aplicación y este se encarga de revisarlo. (Más información en la evidencia)	100%	Reviciones periodicas de cuentas
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	¿Como se da seguimiento al acceso de los usuarios (internos, externos y temporales) y sus actividades en los sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente?	Las repuestas brindadas a los entrevistados: 1. Cada usuario tiene su login y los sistemas permiten ver quien realiza algún cambio. 2.Siempre que se guarde las diferentes acciones con el usuario asignado se puede tener el control de todos los movimientos. Segun la **Politica de accesos a los sistemas informaticos #10.1:** *Cada aplicativo , en la medidad que su diseño lo permita, tendra bitácoras o registros de transacciones efectuadas por uno o más usuarios.*	Las aplicaciones o sistemas, tiene bitácoras o registros de cambios, las cuales pueden revisarse a nivel del aplicación o a nivel de la base de datos.	100%	Registro de actividades en los sistemas de TI
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.	¿Se generan y conservan pistas de auditoría de todos los accesos a la información clasificada como altamente sensible?	Según las repuestas de los entrevistados: Si, en fisico y electronica, tambien en las bitácoras y tablas(basde de datos) queda el registro del usuario en donde se observa fecha, hora y usuario que realiza el cambio.	Las pistas de audioria se conservan en las aplicaciones, en las bases de datos y a nivel fisico, pero solo en caso de modificaciones. No se genera un registro solo por el acceso a la información.	40%	Pistas de auditorias
		Entrevista DSS05.4	**Calificación de la practica DSS05.4:**	82%	L

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	P- >15%-50%	L- >50%-85%	F- >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Tabla N°9. Procesamiento de información en la plantilla DSS05 de práctica DSS05.5

DSS05.05 Gestionar el acceso físico a los activos de TI.

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencias
1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.	¿Cuál es el procedimiento utilizado para las peticiones y concesiones de acceso a las instalaciones de procesamiento de datos?	Debe existir una solicitud , seguida de una autorización y un registro de ingreso. Documentado en la **Politica de administracion fisica y logica de dispositivos y aplicaciones #6.**	La Política de administración física y lógica de la institución **#6.1.2** , menciona que el gerente general tiene que autorizar la lista de personal previamente autorizado, ver registro de ingreso(Evidencia de Actividad 3) no se identifica la firma del gerente general en ninguna de las muestra proporcionada.	**85%**	Peticiones y consesiones de acceso al centro de datos
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	¿Los perfiles de acceso a las ubicaciones de TI están definidos, actualizados y basado de acuerdo con las funciones de trabajo y responsabilidades?	Si, esta definido que solo personal de TI y gerente general tiene acceso al centro de datos, el resto serán visitas de terceros supervisadas	Existe un formato con una lista de personal que están previamente autorizados para el ingreso a las ubicaciones de TI y el resto debe ser registrado y supervisado.	**100%**	Perfiles definidos de Acceso al Centro de datos
3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	¿Se registra y supervisa todos los puntos de entrada a las ubicaciones de TI, incluyendo contratistas y vendedores?	Si, Todos los accesos son supervisados y acompañados por personal de TI. El centro de datos cuenta con registros fotográficos del personal que acceda.	Se logra evidenciar el registro de los accesos al centro de datos .	**100%**	Registro de ingreso al Centro de datos
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	¿De qué manera se instruye al personal para mantener siempre visible su carnet de identificación?	Existe un reglamento interno y un código de vestimenta que indica portar el carnet siempre visible, y jefe de area tiene que asegurar el cumplimiento de esto.	Esta actividad está a cargo el área de capital humano y hay evidencia de que efectivamente se instruye al personal para mantener siempre visible el carnet.	**50%**	Uso de carnet visible
	¿Cómo se previene la expedición de tarjetas o placas de identidad?	RRHH o los jefes de area se encarga de tramitar el carnet de identidad y los accesos electrónicos al area de *Administración de proyectos*	No hay procedimiento formalmente establecido para la expedición de tarjetas de control de entrada a puertas.	**20%**	
5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	¿Se escolta a los visitantes en todo momento durante cualquier actividad que esté llevando a cabo en las ubicaciones de TI?	Los entrevistados coinciden en que si , toda visita es escoltada por personal de TI para evitar accidentes o errores de las visitas.	De acuerdos a las anteriores actividades de esta práctica y según las repuesta de ambos entrevistado se supervisa, escolta y registra a los visitantes.	**100%**	**Ver Actividad 1,2 y 3**
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alarma en caso de acceso no autorizado.	¿Cuáles son las restricciones en el perímetro (como vallas, muros y dispositivos de seguridad) para el acceso a ubicaciones de TI sensibles?	Paredes de gypsum doble tanto desde interior y exterior (4 láminas) puerta de vidrio templado y oscuro acceso mediante tarjetas electrónicas Dispositivo de vigilancia y monitoreo ambiental	Se logra validar las repuestas brindadas.	**50%**	Perimetro y dispositvos que envia alertas,centro de datos
	¿Los dispositivos registran y envian alertas en caso de accesos no autorizados?	Si	Se logró verificar que hay dispositivo que registran y envían alertas.	**50%**	
7. Realizar regularmente formación de concienciación de seguridad física.	¿Realizan actividades regulares de capacitación en sensibilización sobre seguridad física ?	Las repuestas: Si, existe un comité de seguridad de la información donde se abordan estos temas. Los empleados nuevo recibe charla de concientización de la seguridad .	Las repuestas proporcionadas no responden la pregunta. En ninguno de los casos se contempla el tema de seguridad física.	**5%**	**No hay evidencia.**
		Entrevista DSS05.5	**Calificación de la practica DSS05.5:**	**80%**	**L**

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	**P-** >15%-50%	**L-** >50%-85%	**F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Tabla N°10. Procesamiento de información en la plantilla DSS05 de práctica DSS05.6

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencias
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.	¿Cuál es el procedimiento para controlar la recepción, uso, retiro y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa?	De acuerdo a las entrevistas : El procedimiento es abordado en el manual de políticas "*Politica de administración física y lógica de aplicaciones y dispositivos bajo la custodia de TI*" **#4.19 *Desecho de Equipos.***	No hay procedimiento en los documentos de *Politicas* para: La *recepción,uso,retiro y destrucción de formularios especiales.* En la *Politica de administración física y lógica de dispositivos* , a la que hacen referencia solo abarca los temas uso,traslado,reasignacion y desecho de dispositivos.	**15%**	Referencia de documento de la repuesta
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio	¿Se asignan privilegios de acceso a documentos confidenciales y dispositivos de salida, equilibrando riesgo y requerimientos de negocio?	Las repuestas brindadas: **1.** Cada área es dueña de su propia información y el acceso a la misma ya sea de forma física o lógica se administra bajo una matriz de *Key User u Owner Users* (usuario clave o usuario propietario) quienes autorizan o deniegan los accesos de acuerdo con cada rol. **2.** Si,En algunos casos, por ejemplo: • Hay carpetas en servidores donde solo se asigna permiso de acceso (sea de lectura y escritura), según los soliciten los jefes de áreas. • También en SharePoint, cada usuario es responsable de compartir la información con quien estime conveniente. • Las impresoras se les asigna a un PIN para los usuarios que imprimen documentos "confidenciales".	En algunos casos con impresoras y documentos compartidos, se asignan privilegios de accesos según lo solicite o lo estime conveniente el área o departamento responsable de la información. No hay documentación o procedimiento sobre esta actividad.	**40%**	Privilegios de Accesos a Documentos
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	¿Cuenta con un inventario de documentos sensibles y dispositivos de salida, que sea conciliado periódicamente?	Lo que compete a IT, llevamos control del inventario de activos tecnológicos (Hardware, licencias de software) y este es conciliado con el área contable. El área de IT no cuenta con dicho inventario, seria consultar por las distintas áreas si ellos cuentan con un inventario de su documentación sensible.	No hay inventario de documento sensibles. Hay inventario de todos los dispositivos o equipos de TI, incluyendo los dispositivos de salidas y se concilia con el area de contabilidad.	**50%**	Inventario de Equipos de TI,Conciliados
4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	¿Qué medidas de seguridad físicas aplican sobre los documentos especiales y los dispositivos sensibles?	Las respuestas obtenidas en entrevistas: **1.** Los dispositivos sensibles están ubicados en el centro de datos cuyo acceso está limitado a personal debidamente autorizado el cual ingresa al centro mediante control de acceso electrónico. Los Medios de respaldo se manejan en caja de seguridad y en Bóveda de Banco. **2.** Hay una política de seguridad aplicada sobre los dispositivos sensibles, restringiendo el acceso de los mismos según su área y cargo.	Según las repuestas , solo se hace enfasis en las medidas de seguridad fisica para los dispositivos sensibles. En la pregunta anterior se indico que no hay inventario de documentos sensibles.	**50%**	Seguridad Fisica para Dispositivos Sensibles
5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).	¿Cómo se aseguran de destruir la informacion sensible (impresa o medios electronicos) y proteger los dispositivos de salida ? (por ejemplo, desmagnetización de medios electrónicos, destrucción física de dispositivos de memoria, trituradoras)	Las repuestas brindadas: **1.** Algunas áreas cuenta con trituradora de papel y para los medios electronicos se formatea la unidad de almacenamiento. **2.** En las normas y políticas de seguridad hay un artículo donde se indica la destrucción de la información sensible y protección de los dispositivos de salida, los cuales están en resguardo del área de IT	No se logra verificar el uso de trituradoras. Si esta documentado el procedimiento para destruir información electronica. Se protegen con PIN los dispositivos de salidas como impresoras de red (Actividad 2) y bloqueo de memorias USB (DSS05.3)	**50%**	Destruir Información Electronica
		Entrevista DSS05.6	**Calificación de la practica DSS05.6:**	**41%**	**P**

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	**P-** >15%-50%	**L-** >50%-85%	**F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Tabla N°11 Procesamiento de información en la plantilla DSS05 de práctica DSS05.7

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Actividad	Pregunta	Sintesis de las entrevistas y referencia de documentos	Comentarios	Calificación	Evidencias
1. Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	¿Como registran los eventos relacionados con la seguridad que se reportan por las herramientas de monitorización de seguridad de la infraestructura?	Por medio de las alertas emitidas por los dispositivos de monitoreo y en la gran mayoría son enviadas vía correo. También en las oficinas corporativa existe en centro de monitoreo de infraestructura de TI.	Existen herramientas de monitoreo y estas envían los reportes de los eventos a través de correos electrónicos al gerente de IT y Supervisor.	**50%**	Registro de eventos relacionados a la seguridad de la Infraetructura
	De estos registros de Eventos ¿Identifican la información que debe guardarse por un periodo de tiempo apropiado en base a la consideración de riegos?	Todo queda guardada en los correos.	Todo la información de los eventos queda almacenada en los archivos de correo de MS Outlook por tiempo apropiado	**50%**	
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.	¿Cómo definen y comunica la naturaleza y las características de los incidentes potenciales relacionado con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos, para permitir una repuesta apropiada?	Repuestas de los entrevistados: 1. Existe un procedimiento para el tratamiento de incidentes de seguridad de la información. 2. Por correo y por tique se reportan los incidentes, existe un nivel de escalamiento, IT Local, Service Desk corporativo, si el incidente es interno y si no se reporta al respectivo proveedor, y a este nos asigna un tique Según el documento **Politica de seguridad de la información**: **17.1** *Todo incidente de seguridad deberá ser reportado en forma inmediata por el colaborador a HELDESK.Ellos determinaran la acción apropiada a seguir y la prioridad de atención en cada caso.Esto se hara con consultas al jefe/Gerente de IT.* ***17.2*** *HELDESK o su equivalente de Soporte IT en los paises , estan obligados a reportar el incidente en las siguientes 24 horas (o antes según la gravedad) al gerente corporativo de Operaciones y Servicios de IT o al gerente de IT del pais involucrado.*	En resumen el procedimiento es: 1. Reporte del incidente de forma inmediata por correo o por llamada teléfonica al Service Desk 2. Service Desk a su vez reporta a la gerencia de de operaciones de IT (de pais o corporativa según corresponda) y al departamento de seguridad de SITES. 3. Implementar medidas para palear dichos incidentes. 4. Brindar lineamientos para solventar el incidente. 5. Solventar el incidente e informar a los involucrados. *Ver todo el procedimiento en el segmento de evidencias.*	**100%**	Procedimiento para el Tratamiento de incidentes de seguridad de la información
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.	¿Revisan regularmente los registros de eventos para detectar incidentes potenciales?	Si se revisan localmente y existe otros que son monitoreados desde nuestro corporativo.	Si se revisa localmente y desde el centro de monitoreo y control (CMC), que son los encargados de revisar los eventos de incidentes de la infraestructura.	**100%**	**Ver Actividad 1**
4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	¿Cuentan con un procedimiento para la recopilación de evidencia en linea de acuerdo con las reglas locales de evidencia forense y aseguran de que todo el personal esté al tanto de los requisitos?	No	No existe el procedimiento para la recopilacion de evidencia en linea.	**0%**	**N.A**
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	¿Los tiques de incidentes de seguridad se crean de manera oportuna cuando la monitorización identifica posibles incidentes de seguridad?	Si, también esta detallado en el procedimiento (***Tratamiento de incidentes de la información***), la generación del tique de manera inmediata.	Se verifico la creación de tiques de manera oportuna, cuando se presentan incidentes.	**100%**	Tiques creados de manera oportuna
		Entrevista DSS05.7	**Calificación de la practica DSS05.7:**	**80%**	**L**

Califiación de la Practica= (∑Calificación)/(№ Actividades)

N- 0%-15%	**P-** >15%-50%	**L-** >50%-85%	**F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Resultado Final de la Evaluación

Tabla N°12.Calificaciones de las 7 prácticas de gestión

DSS05 Gestionar Servicios de Seguridad		Calificación
DSS05.01	Proteger contra software malicioso	77%
DSS05.02	Gestionar la seguridad de la red y las	51%
DSS05.03	Gestionar la seguridad de los puestos de usuario final.	84%
DSS05.04	Gestionar el acceso físico a los activos de	82%
DSS05.05	Gestionar documentos sensibles y dispositivos de salida.	80%
DSS05.06	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	41%
DSS05.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	80%
	Grado de cumplimiento del proceso:	71%

Grado de cumplimiento del proceso:= ∑Calificación de las practicas **/** 7 (№ Practicas)

Gráfico N°1. Calificaciones de las prácticas de gestión del proceso

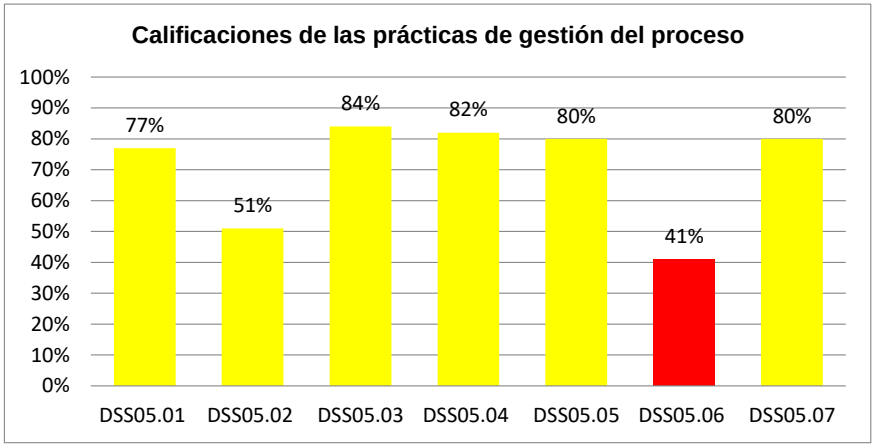


Tabla N°13. Nivel de capacidad obtenido para el proceso

Nombre del proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
DSS05		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Escala de calificación		L								
Escala de porcentaje		71%								

Comentarios :
Como resultado de la evaluación del proceso DSS05: Gestionar servicios de seguridad de COBIT 5.0, usando la metodología de las capacidades y madurez de la norma ISO / IEC 15504, se determina el nivel capacidad **1(Realización del proceso)** con una calificación **71% , L- Ampliamente Conseguido.**

Debido a que el proceso no obtuvo calificación "Totalmente Conseguido" para el atributo PA1.1 , no es posible evaluar los atributos del nivel de capacidad superior (PA2.1 y 2).

N- 0%-15%	P- >15%-50%	L- >50%-85%	F- >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

4.4 Debilidades y Hallazgos

DSS05.01 Proteger contra software malicioso (malware).

No hay documentación, ni procedimientos formalmente establecido para la actividad de concientizar sobre software malicioso y para la prevención.

Falta un programa de capacitación en temas de malware en el correo electrónico, uso de internet y software no autorizados.

DSS05.02 Gestionar la seguridad de la red y las conexiones.

Carencia de una evaluación de riesgos alineada al negocio.

Los puntos de conexión a la red de la empresa son una vulnerabilidad, al igual que el acceso a internet sin restricciones de algunos usuarios.

No hay herramienta encriptar la información en transito

No se realiza ningún tipo de pruebas de intrusión, tampoco pruebas que determinen la protección de los sistemas de información.

El uso de protocolo inseguro como telnet.

DSS05.03 Gestionar la seguridad de los puestos de usuario final.

No se encontró un plan a ejecutar para el mantenimiento preventivo de equipos de usuario final.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

No hay una clasificación de seguridad para los accesos a los activos de información

Se generan pistas de auditorías de las modificaciones, pero no de los accesos a la información.

DSS05.05 Gestionar el acceso físico a los activos de TI.

No se encontró procedimiento formal para la expedición de tarjetas de control de entrada a puertas.

El control del acceso a las puertas de las ubicaciones de TI, en especial la del cuarto de procesamiento de información está administrado por otra área que no es TI.

No se realizan actividades regulares de capacitación sobre la seguridad física.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

No existe procedimiento para controlar la recepción, uso, retiro y destrucción de formularios especiales y dispositivos de salida

No hay procedimientos establecidos para asignación de privilegios de acceso a documentos confidenciales y dispositivos de salidas.

No hay inventario, ni medidas de seguridad físicas para los documentos sensibles

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

No hay procedimiento para la recopilación de evidencia en línea de acuerdo con las reglas locales de evidencia forense.

4.5 Fortalezas

DSS05.01 Proteger contra software malicioso (malware).

Una excelente y completa herramienta Antimalware (Administración, Configuración y distribución centralizada, Actualizaciones automáticas)

Herramienta de respaldo de información automático para los usuarios claves

DSS05.02 Gestionar la seguridad de la red y las conexiones.

Contar con firewall y herramienta de filtrado de contenido web

DSS05.03 Gestionar la seguridad de los puestos de usuario final.

Excelentes mecanismos de bloqueo para dispositivos de usuarios final

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

Política más procedimientos formales para el proceso de altas, bajas y cambios de acceso a los sistemas de información.

Buena gestión y separación de los accesos privilegiados

DSS05.05 Gestionar el acceso físico a los activos de TI.

Procedimiento formal de para el ingreso a centro de datos.

Buena infraestructura en el centro de datos (paredes reforzadas, dispositivos de vigilancia y monitoreo, puerta de vidrio templado y oscuro, aire de precisión, piso forrado con Alfombra antiestática)

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

Para esta práctica no determinamos ninguna fortaleza

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Se cuenta con herramientas de monitoreo de la infraestructura de TI, también un centro de monitoreo dividido por áreas como redes, bases de datos y operaciones.

Generación de ticket de manera oportuna por un Service Desk y un apropiado nivel de escalamiento.

4.6 Costos del diagnóstico de la seguridad de la información con DSS05

Los costos se calculan en base a las fases que se realizan en la formulación y ejecución de la evaluación, cada una de estas fases con sus propias actividades.

Duración = 3 meses.
Tiempo = 3 días a la semana, 4 horas por días.

Tabla N° 14 Costos de la evaluación

COSTOS DE LA EVALUACION DE LA SEGURIDAD DE LA INFORMACION PARA UNICOMER NICARAGUA			
FASES QUE REALIZAR	*COSTO X FASE*	*TIEMPO DE TRABAJO (4h x día)*	*COSTO TOTAL*
PREPARACION DE ESTUDIO	*$20 x hora*	*3 días*	*240.00*
RECOPILACION DE LA INFORAMCION	*$ 25 x hora*	*18 días*	*1800.00*
PROCESAMIENTO DE LA INFORMACION	*$25 x hora*	*15 días*	*1, 500. 00*
EVALUACION	*$ 25 x hora*	*7 días*	*700.00*
REALIZACION DE INFORME DE AUDITORIA	*$20 x hora*	*1 día*	*80.00*
Evaluador	*Carlos Ortiz*		
	Costos totales		*$ 4, 320.00*

El costo total de la implementación de esta auditoria es de $ 4, 320.00 (cuatro mil trescientos veinte dólares americanos).

CAPITULO V:

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Este estudio muestra cómo se puede realizar una evaluación en una empresa haciendo uso de COBIT, los objetivos propuestos en la monografía se cumplieron completamente además de desarrollarse un instrumento de registro, procesamiento y presentación de resultados auxiliado de Microsoft Excel.

UNICOMER tiene la oportunidad de mejorar sus prácticas a corto plazo por cuanto tiene un nivel cumplimiento de 71%, pudiendo desarrollar en su totalidad las prácticas de gestión como DSS05.3 Y DSS05.4 que obtuvieron un grado de cumplimiento de 84 % y 82 % respectivamente. De manera general podemos concluir que la empresa obtuvo un resultado Aceptable (Ampliamente conseguido).

Las prácticas de gestión que necesitan más atención son: DSS05.2 Gestionar la seguridad de la red y las conexiones y DSS05.2 Supervisar la infraestructura para detectar eventos relacionados a la seguridad, donde estas 2 prácticas son las que obtuvieron un grado de cumplimiento muy bajo.

Debido a que el proceso no obtuvo calificación "Totalmente Conseguido" para el atributo PA1.1, no es posible evaluar los atributos del nivel de capacidad superior (PA2.1 y 2).
De dar seguimientos a las debilidades y si llegasen a superarse siguiendo las recomendaciones brindadas, en una siguiente evaluación del proceso es muy probable que se obtenga un grado de capacidad o madurez de nivel 2 gestionado.

Limitaciones : Aunque contamos con el apoyo del gerente de TI, quien nos brindó su confianza para hacer posible el desarrollo de la evaluación, consideramos que no se tuvo acceso a toda la información de la compañía, porque consideraban que podría exponer información sensible de la misma y por otra parte hay información que es administrada por su corporativo, principalmente el estudio se desarrolló por la entrevista y en un menor grado verificaciones y revisión documental.

5.2 Recomendaciones

Es necesario cubrir y poner atención a las actividades que obtuvieron calificación menor al 50% en la evaluación del proceso DSS05, para que la empresa cubra todas sus debilidades evaluando cuál de ellas son las más urgentes.

Detallamos algunas recomendaciones para cubrir las debilidades encontradas:

- Definir procedimientos para concientizar sobre la prevención del software malicioso y establecer un programa de capacitación específicamente en temas de malware, uso de internet, correo y el uso del internet.
- Elaborar un análisis de riesgos alineados al negocio y que este sea tomado en cuentas en las políticas de seguridad de TI.
- Valorar la vulnerabilidad de acceso a la red y el internet con la implementación de revisiones de posibles accesos no autorizados a la red, para determinar la protección de los sistemas de información, también cambiar el protocolo de conexión remota telnet por el protocolo Secure Shell(SSH).
- Establecer y mantener un procedimiento para la expedición de tarjetas electrónicas de acceso a las instalaciones y valorar la posibilidad de independizar la administración y control de acceso de las ubicaciones de TI.
- Realizar procedimiento para para asignación de privilegios de acceso a documentos confidenciales, dispositivos de salida, a su vez para controlar la recepción, uso, retiro y destrucción de formularios especiales.
- Establecer una clasificación de seguridad para los accesos a los activos de información, valorar la implementación de herramientas para encriptar la información almacenada y tránsito.

5.3 Glosario

A

Activo: Son aquellos recursos (hardware y software) con los que cuenta una empresa. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.

Antimalware: Es un tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI. Los términos antivirus y antimalware se utilizan a menudo como sinónimos ya que los virus informáticos son un tipo específico de malware.

C

Componentes: Es aquello que forma parte de la composición de un todo. Se trata de elementos que, a través de algún tipo de asociación o contigüidad, dan lugar a un conjunto uniforme.

Cobit: (objetivos de control para la información y tecnología). Es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Cortafuegos: (Firewall), es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

E

Estándares: Los estándares son acuerdos (normas) documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características. Para asegurar que los materiales productos, procesos y servicios se ajusten a su propósito.

F

Framework: En el desarrollo de software, un framework es una estructura conceptual y tecnológica de soporte definida, normalmente con artefactos o módulos de software concretos, en base a la cual otro proyecto de software puede ser organizado y desarrollado.

H

Https: Abreviatura de la forma inglesa Hypertext Transfer Protocol, 'protocolo de transferencia de hipertextos', que se utiliza en algunas direcciones de internet.

I

ISACA: es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

ISO/IEC 15504: También conocido como Software Process Improvement Capability Determination, abreviado SPICE, en español, «Determinación de la Capacidad de Mejora del Proceso de Software» es un modelo para la mejora, evaluación de los procesos de desarrollo, mantenimiento de sistemas de información y productos de software.

M

Malware: Es la abreviatura de Malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de Malwares podemos encontrar términos como por ejemplo, Virus, Troyanos, Gusanos (Worm), keyloggers, Botnets.

O

Outsourcing: Es el proceso económico empresarial en el que una sociedad mercantil transfiere los recursos y las responsabilidades referentes al cumplimiento de ciertas tareas a una sociedad externa, empresa de gestión o información.

Owner user: Usuario propietario, persona responsable del proceso de gestión de accesos, a nivel del área de negocio, en la cual el sistema informático es utilizado. Crea y da mantenimiento a la matriz de decisión de roles relacionado a su aplicación.

P

Phishing: Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

Protocolos: Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

Proxy: O servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).

Protocolos de seguridad: Es un conjunto de intercambios en los que intervienen normalmente dos o tres entidades: La entidad iniciadora del protocolo (entidad a), la entidad receptora (entidad b) y una tercera entidad opcional (entidad c) con la

misión de autenticación de los intercambios, distribución de claves públicas y/o claves de sesión.

S

Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

SSH: Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.

Service Desk: Conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación.

T

TIC: Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro.

U

Usuario final: En informática, es la persona para la que está diseñado un software o un dispositivo de hardware.

5.4 Bibliografía

[1] Excellence, I. (05 de 2015). Sistema de Gestión de Seguridad de la Información. Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[2] ISACA Journal. (2015). Select COBIT 5 Processes for Essential Enterprise Security Obtenido de https://www.isaca.org/Journal/archives/2015/Volume-2/Pages/selected-cobit-5-processes-for-essential-enterprise-security.aspx

[3] Objetivos de control para la información y tecnologías relacionadas. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas

[4] ISACA. (s.f.). Obtenido de https://www.isaca.org/Groups/Professional-English/cobit-5-use-it-effectively/Pages/ViewDiscussion.aspx?PostID=18

[5] 20minutos Tecnologia . (23 de Noviembre de 2011). Obtenido de Tipos de malware : https://listas.20minutos.es/lista/los-tipos-de-malware-310619/

[6] Evaluación del nivel de capacidad de los procesos de TI, mediante el marco de referencia COBIT PAM. (s.f.). Obtenido de https://www.researchgate.net/publication/317558763_Evaluacion_del_nivel_de_capacidad_de_los_procesos_de_TI_mediante_el_marco_de_referencia_COBIT_PAM

[7] Celi, Ernesto. (2017). Evaluación del nivel de capacidad de los procesos de TI, mediante el marco de referencia COBIT PAM.

[8] Glone A. (02 de Jan de 2011). Gestión de acceso de usuario. Obtenido de https://iso27002.wiki.zoho.com/11-2-Gesti%C3%B3n-de-acceso-de-usuario.html

[9] ISACA JOURNAL. (12 de 04 de 2012). Obtenido de Evaluación de la capacidad y/o madurez de los procesos: https://www.isaca.org/Groups/Professional-English/cobit-5-use-it-effectively/Pages/ViewDiscussion.aspx?PostID=18

[10] ISACA Journal volumen 1. (2016). Obtenido de como COBIT 5 mejora la capacidad de procesos de trabajo de auditores, profesionales de aseguramiento y evaluadores: https://www.isaca.org/Journal/archives/2016/Volume-1/Pages/how-cobit-5-improves-the-work-process-capability-of-auditors-spanish.aspx#8

[11] ISACA. (2012). COBIT5 - Procesos Catalizadores. Rolling Meadows, IL 60008 EE.UU.pp.191-195

CAPITULO VI: ANEXOS

Anexo 1. Cuestionarios formulados.

Cuestionario de evaluación C1

DSS05.01 Proteger contra software malicioso (malware)

1. **¿Cómo se concientiza sobre software malicioso?**

   Respuesta A:
   Repuesta B:

2. **¿Cómo se refuerza los procedimientos preventivos y responsabilidades sobre software malicioso?**

   Repuesta A:
   Repuesta B:

3. **¿Qué herramientas son activadas para proteger en contra de software malicioso?**

   Repuesta A:
   Repuesta B:

4. **¿Cómo se actualiza el software antivirus y las definiciones de software malintencionados (Automática o Semiautomática)?**

   Repuesta A:
   Repuesta B:

5. **¿Cómo distribuyen todo el software de protección? ¿Es centralizado?**

   Repuesta A:
   Repuesta B:

6. **¿Cómo se gestiona el cambio y configuración de software de protección?**

   Repuesta A:
   Repuesta B:

7. **¿Cómo se revisa y evalúa periódicamente la información sobre nuevas potenciales amenazas de malware? (Ejemplos: Revisando productos de proveedores y servicios de alertas de seguridad)**

   Repuesta A:
   Repuesta B:

8. **¿Cómo se filtra el tráfico entrante de internet, para evitar correos de phishing y descargas de software espías?**

   Repuesta A:
   Repuesta B:

9. **¿Cómo educan y capacitan a los usuarios respecto al tema de malware en el correo electrónico, el uso del internet y el no instalar software no autorizado?**

   Repuesta A:
   Repuesta B:

Cuestionario de evaluación C2

DSS05.02 Gestionar la seguridad de la red y las conexiones.

1. **¿En función de las evaluaciones de riesgos y los requisitos del negocio, cuentan con una política de seguridad de las conexiones?**

   Repuesta A:
   Repuesta B:

2. **¿Cómo se garantiza y controla que solo los dispositivos autorizados tengan acceso a la información y a la red empresarial?**

   Repuesta A:
   Repuesta B:

3. **¿Se configura estos dispositivos para que solicite contraseña?**

   Repuesta A:
   Repuesta B:

4. **¿Con qué mecanismos de filtrado de red cuentan (¿Firewall, Software de detección de intrusos?**

   Repuesta A:
   Repuesta B:

5. **En estos mecanismos ¿cuáles son las políticas configuradas que se consideran más importantes para el filtrado de tráfico entrante y saliente?**

   Repuesta A:
   Repuesta B:

6. ¿La información en tránsito está encriptada de acuerdo con su clasificación?

Repuesta A:
Repuesta B:

7. ¿A nivel de conectividad que protocolos de seguridad se utilizan?

Repuesta A:
Repuesta B:

8. ¿Se configuran los equipos de red de forma segura?

Repuesta A:
Repuesta B:

9. ¿Cuáles son los parámetros de seguridad configurados en los equipos activos de red (Enrutadores, Conmutadores, Puntos de acceso)?

Repuesta A:
Repuesta B:

10. ¿Qué mecanismos de confianza se establecen para dar soporte a la transmisión y recepción segura de la información?

Repuesta A:
Repuesta B:

11. ¿Realizan pruebas de intrusión (“Ethical Hacking”) para determinar el nivel de protección de la red? ¿Con que frecuencia?

Repuesta A:
Repuesta B:

12. ¿Realizan pruebas periódicas para determinar la adecuación de la protección de los sistemas de información?

Repuesta A:
Repuesta B:

Cuestionario de evaluación C3

DSS05.03 Gestionar la seguridad de los puestos de usuario final.

1. **¿Qué actividades realizan hacer más seguros los sistemas operativos y reducir las vulnerabilidades?**

   Repuesta A:
   Repuesta B:

2. **¿Cuáles son los mecanismos de bloqueo que se implementan en los dispositivos del usuario final?**

   Repuesta A:
   Repuesta B:

3. **¿Se cifra la información almacenada en los dispositivos, de acuerdo con su clasificación?**

   Repuesta A:
   Repuesta B:

4. **¿Cómo se gestiona el acceso remoto y control de los equipos de usuario final?**

   Repuesta A:
   Repuesta B:

5. **¿Cómo administran la configuración de red de forma segura en los dispositivos de los usuarios?**

   Repuesta A:
   Repuesta B:

6. **¿Se implementa el filtrado del tráfico en la red, en dispositivos de usuario final? ¿Cómo?**

   Repuesta A:
   Repuesta B:

7. **¿Cómo protegen la integridad de los sistemas operativos?**

   Repuesta A:
   Repuesta B:

8. **¿Cuáles son las medidas de protección a nivel físico con la que cuentan los dispositivos de usuario final?**

   Repuesta A:
   Repuesta B:

9. **¿Cuál es el procedimiento para desechar los dispositivos de usuario final de forma segura?**

   Repuesta A:
   Repuesta B:

Cuestionario de evaluación C4

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

1. **¿Los accesos otorgados a cada usuario en los diferentes aplicativos son de acuerdo con el rol y la función definidos para la unidad de negocio correspondiente?**

   Repuesta A:
   Repuesta B:

2. **¿Se alinea la asignación de roles, funciones y responsabilidades definidas en los sistemas, basándose en los principios de menor privilegio?**

   Repuesta A:
   Repuesta B:

3. **¿Se identifica de manera única todas las actividades de procesamiento de información por roles?**

   Repuesta A:
   Repuesta B:

4. **¿Coordinan los roles con las unidades del negocio y aseguran que todos los roles están definidos consistentemente, incluyendo los roles definidos por el propio negocio?**

   Repuesta A:
   Repuesta B:

5. **Basándose en su clasificación de seguridad ¿Se autentica todo acceso a los activos de información y asegurando que los controles de autenticación han sido administrados adecuadamente?**

   Repuesta A:
   Repuesta B:

6. **¿Cómo se manejan las altas, bajas y cambios de accesos en los sistemas de información?**

Repuesta A:
Repuesta B:

7. **Esta gestión de acceso ¿Son las transacciones aprobadas, documentadas y autorizadas?**

   Repuesta A:
   Repuesta B:

8. **¿Cómo se gestionan y separan los niveles de acceso privilegiado?**

   Repuesta A:
   Repuesta B:

9. **¿Realizan revisiones periódicas de la gestión de todas las cuentas y niveles de privilegios relacionados?**

   Repuesta A:
   Repuesta B:

10. **¿Cómo se da seguimiento al acceso de los usuarios (internos, externos y temporales) y sus actividades en los sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente?**

    Repuesta A:
    Repuesta B:

11. **¿Se generan y conservan pistas de auditoría de todos los accesos a la información clasificada como altamente sensible?**

    Repuesta A:
    Repuesta B:

Cuestionario de evaluación C5

DSS05.05 Gestionar el acceso físico a los activos de TI.

1. **¿Cuál es el procedimiento utilizado para las peticiones y concesiones de acceso a las instalaciones de procesamiento de datos?**

   Repuesta A:
   Repuesta B:

2. **¿Los perfiles de acceso a las ubicaciones de TI están definidos, actualizados y basado de acuerdo con las funciones de trabajo y responsabilidades??**

   Repuesta A:
   Repuesta B:

3. **¿Se registra y supervisa todos los puntos de entrada a las ubicaciones de TI, incluyendo contratistas y vendedores?**

   Repuesta A:
   Repuesta B:

4. **¿De qué manera se instruye al personal para mantener siempre visible su carnet de identificación?**

   Repuesta A:
   Repuesta B:

5. **¿Cómo se previene la expedición de tarjetas o placas de identidad?**

   Repuesta A:
   Repuesta B:

6. **¿Se escolta a los visitantes en todo momento durante cualquier actividad que esté llevando a cabo en las ubicaciones de TI?**

   Repuesta A:
   Repuesta B:

7. **¿Cuáles son las restricciones en el perímetro (como vallas, muros y dispositivos de seguridad) para el acceso a ubicaciones de TI sensibles?**

   Repuesta A:
   Repuesta B:

8. **¿Los dispositivos registran y envían alertas en caso de accesos no autorizados?**

   Repuesta A:
   Repuesta B:

9. **¿Realizan actividades regulares de capacitación en sensibilización sobre seguridad física?**

   Repuesta A:

   Repuesta B:

Cuestionario de evaluación C6

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

1. **¿Cuál es el procedimiento para controlar la recepción, uso, retiro y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa?**

   Repuesta A:
   Repuesta B:

2. **¿Se asignan privilegios de acceso a documentos confidenciales y dispositivos de salida, equilibrando riesgo y requerimientos de negocio?**

   Repuesta A:
   Repuesta B:

3. **¿Cuenta con un inventario de documentos sensibles y dispositivos de salida, que sea conciliado periódicamente?**

   Repuesta A:
   Repuesta B:

4. **¿Qué medidas de seguridad físicas aplican sobre los documentos especiales y los dispositivos sensibles?**

   Repuesta A:
   Repuesta B:

5. **¿Cómo se aseguran de destruir la información sensible (impresa o medios electrónicos) y proteger los dispositivos de salida?**
   (Por ejemplo, des magnetización de medios electrónicos, destrucción física de dispositivos de memoria, trituradora)

   Repuesta A:
   Repuesta B:

Cuestionario de evaluación C7

DSS05.07 Supervisar la infraestructura para detectar eventos

1. **¿Cómo registran los eventos relacionados con la seguridad que se reportan por las herramientas de monitorización de seguridad de la infraestructura?**

   Repuesta A:
   Respuesta B:

2. **De estos registros de Eventos ¿Identifican la información que debe guardarse por un periodo de tiempo apropiado en base a la consideración de riegos?**

   Repuesta A:
   Respuesta B:

   ¿Cómo se define y comunica la naturaleza y las características de los incidentes potenciales relacionado con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos, para permitir una repuesta apropiada?

   Repuesta A:
   Respuesta B:

3. **¿Revisan regularmente los registros de eventos para detectar incidentes potenciales?**

   Repuesta A:
   Repuesta B:

4. **¿Cuentan con un procedimiento para la recopilación de evidencia en línea de acuerdo con las reglas locales de evidencia forense y aseguran de que todo el personal esté al tanto de los requisitos?**

   Repuesta A:
   Repuesta B:

5. **¿Los tiques de incidentes de seguridad se crean de manera oportuna cuando la monitorización identifica posibles incidentes de seguridad?**

   Repuesta A:
   Repuesta B:

Anexo 2. Cuestionarios Completados

Cuestionario de evaluación C1

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.01 Proteger contra software malicioso (malware)		
Entrevistado A:	Alvaro Zeledon	**Cargo:**	Gerente de TI
Entrevistado B:	Silver Mora	**Cargo:**	Técnico de soporte y Helpdesk
Entrevistado C:	Maria Arguello	**Cargo:**	Asistente gerencia Capital Humano

1. ¿Cómo se concientiza sobre software malicioso?

Respuesta A:
Se envían boletines informativos a través de correo electrónico a todo el personal y cuando es una situación general para toda la región envían correos desde el corporativo desde una cuenta llamada *Informativo Seguridad IT*

Repuesta B:
Se le envía a Capital humano el correo y ellos a través de una cuenta que se llama *comunicación interna NIC* (Pregunta 2) envían el correo masivo.

Entrevista con responsable de envió de comunicaciones internas.
¿Cómo funciona el envío de correos desde la cuenta *Comunicación Interna NIC*?

Repuesta C:
Todas las comunicaciones con información pública (por así decirlo), de las diferentes áreas las enviamos por medio de esta cuenta, con copia oculta (CCo), para que la gente no le de **Responder a todos,** se envía a todos los grupos que aplique la comunicación, por lo general la mayoría de los comunicados es para todos, en ocasiones solo Oficinas.

2. ¿Cómo se refuerza los procedimientos preventivos y responsabilidades sobre software malicioso?

Repuesta A:
El procedimiento es preparar toda computadora con las herramientas para la prevención de software malicioso (Antivirus, Parches de seguridad), hay un check list para preparar un equipo antes de entregarla al usuario que va a ser responsable de este.

Repuesta B:
Nosotros (técnicos de soporte) preparamos el equipo con las aplicaciones, tenemos una imagen de sistema operativo con los programas que no pueden faltar *(Antivirus, SCCM, Agente OCS, Winrar, Parches de seguridad y otras aplicaciones que se utilizan casi en todos los equipos)*, hasta este punto es responsabilidad de nosotros, después el usuario queda de responsable del equipo.

3. ¿Qué herramientas son activadas para proteger en contra de software malicioso?

Repuesta A:
Antivirus (McAfee VirusScan Enterprise)

Repuesta B:
McAfee VirusScan Enterprise + AntiSpyware Enterprise
McAfee DLP Endpoint para desactivar el uso memorias USB
Herramientas de respaldo automático para usuario claves.

4. ¿Cómo se actualiza el software antivirus y las definiciones de software malintencionados (Automática o Semiautomática)?

Repuesta A:
Por medio de repositorio central de antivirus que distribuye todas las actualizaciones de antivirus de forma automática.

Repuesta B:
Todas la maquinas se preparan con el agente de McAfee este tiene parametrizado la conexión con el servidor de donde toma las actualizaciones.

5. ¿Cómo distribuyen todo el software de protección? ¿Es centralizado?

Repuesta A:
Por medio *System Center Configuration Manager* (SCCM) y *Active Directory* (AD) se programan tareas de despliegue automático.

Repuesta B:
Todas las maquinas cuando se entregan van con el antivirus, pero cuando hay que instalar actualizaciones del agente de McAfee se hace un despliegue por medio de *SCCM*, y también tenemos una herramienta que se llama *OCS Inventory.*

6. ¿Cómo se gestiona el cambio y configuración de software de protección?

Repuesta A:
Con la consola de *McAfee ePolicy Orchestrator* (McAfee ePO)

Repuesta B:
Todos los cambios y configuraciones se realizan desde la consola de administración de McAfee.

7. ¿Cómo se revisa y evalúa periódicamente la información sobre nuevas potenciales amenazas de malware? (Ejemplos: Revisando productos de proveedores y servicios de alertas de seguridad)

Repuesta A:
Existe un comité de seguridad de TI que se mantiene en constante monitoreo e investigación sobre nuevas potenciales amenazas y nuevos productos o soluciones de seguridad.

Repuesta B:
Existe un comité de seguridad, ellos están encargados de esta tarea.

8. ¿Cómo se filtra el tráfico entrante de internet, para evitar correos de phishing y descargas de software espías?

Repuesta A:
El McAfee se integra con el Outlook y él se encarga de la seguridad en los correos.

Repuesta B:
McAfee analiza la recepción de correo electrónico y también tiene directivas de programas no deseados.

9. ¿Cómo educan y capacitan a los usuarios respecto al tema de malware en el correo electrónico, el uso del internet y el no instalar software no autorizadas?

Repuesta A:
En coordinación con el área de capital Humano, TI imparte charlas de las políticas de seguridad de la información y políticas generales de TI. También por comunicaciones internas se envían recomendaciones, boletines informativos y las políticas de seguridad.

Repuesta B:
A los colaboradores de nuevo ingreso en la inducción se les da una charla de las políticas de seguridad de la información y abarcan estos temas.

Cuestionario de evaluación C2

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.02 Gestionar la seguridad de la red y las conexiones.		
Entrevistado A:	Alvaro Zeledon	**Cargo:**	Gerente de TI
Entrevistado B:	Silver Mora	**Cargo:**	Técnico de soporte y Helpdesk

1. ¿En función de las evaluaciones de riesgos y los requisitos del negocio, cuentan con una política de seguridad de las conexiones?

Repuesta A:
En la *política de seguridad de información* del grupo, tenemos políticas de las conexiones, como acceso a red, uso de correo, red inalámbrica, internet y a nivel de país se está trabajando en una matriz de riesgos y alinear al país la política actual. (No va a cambiarse de Política)

Repuesta B:
Si, la Política que se tiene es la misma para toda la región y está en función del negocio, desconozco si está en función de los riesgos.

2. ¿Cómo se garantiza y controla que solo los dispositivos autorizados tengan acceso a la información y a la red empresarial?

Repuesta A:
Sí, todos los dispositivos de red y sistemas de información solicitan credenciales de acceso y autenticación.

Repuesta B:
Para el acceso a la información todos los sistemas de información se solicitan credenciales de acceso, incluso para ingresar a Windows. Para ingreso a red por WIFI solicita usuario y contraseña, pero por cable no hay restricción.

3. ¿Se configura estos dispositivos para que solicite contraseña?

Repuesta A:
Sí, todos los dispositivos de red solicitan credenciales de acceso y autenticación.

Repuesta B:
Si, para ingresar a la configuración de los equipos todos se le configuran contraseña.

4. ¿Con qué mecanismos de filtrado de red cuentan (¿Firewall, Software de detección de intrusos)?

Repuesta A:
Hay un Firewall Cisco ASA

Repuesta B:
Firewall
Servidor proxy para el filtrado de internet.

5. En estos mecanismos ¿cuáles son las políticas configuradas que se consideran más importantes para el filtrado de tráfico entrante y saliente?

Repuesta A:

•El permitir las redes de la empresa y seguras
•Bloquear los puertos de conexión y permitir solo los aprobados o seguros.
•Para lo de salida está el proxy para que el usuario no tenga acceso total a internet

Repuesta B:

Acceso a los segmentos de redes de la empresa y a direcciones IP públicas de empresas de confianza (ejemplo: central de riesgo, bancos) y bloquear el acceso las demás redes.

6. ¿La información en tránsito está encriptada de acuerdo con su clasificación?

Repuesta A:

No

Repuesta B:

No

7. ¿A nivel de conectividad que protocolos de seguridad se utilizan?

Repuesta A:

HTTPS, SSH, VPN (IP SEC), SSL

Repuesta B:

SSH, HTTPS, SSL

8. ¿Se configuran los equipos de red de forma segura?

Repuesta A:

Si

Repuesta B:

Lo esencial, usuario, contraseña, cantidad de intentos

9. ¿Cuáles son los parámetros de seguridad configurados en los equipos activos de red (Enrutadores, Conmutadores, Puntos de acceso)?

Repuesta A:

Usuario, contraseña, tiempo para desconectase si no hay actividad, utilizar protocolos de conexión segura SSH

Repuesta B:

Usuario y contraseña, 3 intentos de conexión, 30 segundos sin actividad y se cierra la sesión, esto para los equipos de las sucursales.

10. ¿Qué mecanismos de confianza se establecen para dar soporte a la transmisión y recepción segura de la información?

Repuesta A:

- Proxy (Filtrado WEB)
- Protocolos Seguros (SSL, SSH, HTTPS)
- Firewall
- Antivirus (McAfee Enterprise)
- Políticas de grupo en Active Directory

Repuesta B:

Se utiliza VPN
Contamos con un Firewall
Filtrado de acceso a internet para los usuarios.
Bloqueo de envió de correos a dominios externos

11. ¿Realizan pruebas de intrusión ("Ethical Hacking") para determinar el nivel de protección de la red? ¿Con que frecuencia?

Repuesta A:

No

Repuesta B:

Desde que laboro acá nunca han hecho eso.

12. ¿Realizan pruebas periódicas para determinar la adecuación de la protección de los sistemas de información?

Repuesta A:

No, Solo pruebas que solicita auditoria y pruebas de restauración de bases de datos.

Repuesta B:

No

Cuestionario de evaluación C3

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.03 Gestionar la seguridad de los puestos de usuario final.		
Entrevistado A:	Alvaro Zeledón	**Cargo:**	Gerente de TI
Entrevistado B:	Silver Mora	**Cargo:**	Técnico de soporte y HelpDesk

1. ¿Qué actividades realizan hacer más seguros los sistemas operativos y reducir las vulnerabilidades?

Repuesta A:
Desinstalar todas las aplicaciones que vienen de fábrica.
Instalar Software Antivirus.
Se aplican políticas de grupo por Active Directory
Los usuarios no tienen permisos de administración del sistema operativo.

Repuesta B:
Instalar Antivirus
Instalar aplicaciones de acuerdo con el perfil laboral del usuario.
Los usuarios de Windows se dejan como estándar.
Bloqueo de los puertos USB
Se quitan aplicaciones del inicio de Windows.

2. ¿Cuáles son los mecanismos de bloqueo que se implementan en los dispositivos del usuario final?

Repuesta A:
Cuando el equipo queda inactivo por 5 minutos se bloquea automáticamente.
Luego de 10 intentos fallidos se bloquea la cuenta de usuario.
Las portátiles se le colocan contraseña de arranque (BIOS) y de disco duro.
Usuarios que se les asignan celular es exigido utilizar contraseña.

Repuesta B:
Autenticación en Active Directory (AD), con cantidad limitada de intentos.
Computadoras Portátiles se coloca contraseña de hardware y de disco duro, también se brinda cables de seguridad.

3. ¿Se cifra la información almacenada en los dispositivos, de acuerdo con su clasificación?

Repuesta A:
Discos duros externos se cifran con BitLocker y los discos duros de portátil se colocan contraseña a nivel de BIOS.
Si, por lo general los usuarios de portátil, son los usuarios que manejan información importante.

Repuesta B:
Hay ciertos usuarios que se les brinda discos duros externos para realicen respaldo de su información, y estos se cifran colocando contraseña.

4. ¿Cómo se gestiona el acceso remoto y control de los equipos de usuario final?

Repuesta A:
Se instala una aplicación llamada VNC server y cuando el usuario necesita apoyo se solicita su dirección IP.
Pocos casos se usa escritorio remoto y conexión por SCCM.

Repuesta B:
Todas las computadoras al prepararse se le instala el programa *VNC Server*, se le configura una contraseña y nosotros (Técnicos) tenemos el *VNC Viewer*, cuando un usuario necesita asistencia, le solicitamos la dirección IP y así tenemos el control del equipo.

5. ¿Cómo administran la configuración de red de forma segura en los dispositivos de los usuarios?

Repuesta A:
Todos los colaboradores con computadora pueden acceder a la intranet. Sin embargo, para los accesos a internet existen perfiles de navegación preestablecidos (grupos de páginas web) de acuerdo con el rol del colaborador. (*Ver política de acceso y seguridad de la información*)

Repuesta B:
Todas las computadoras tienen acceso a la red local y para acceso a sitios de internet por política de grupo se le asigna un grupo de navegación según el perfil laboral del usuario y así poder acceder a las páginas que necesita.

6. ¿Se implementa el filtrado del tráfico en la red, en dispositivos de usuario final? ¿Cómo?

Repuesta A:
Si, mediante proxy.

Repuesta B:
Todas las PC de escritorio usan proxy, para limitar la navegación en internet. El usuario de portátil con acceso a las redes inalámbrica tiene acceso libre en internet.

7. ¿Cómo protegen la integridad de los sistemas operativos?

Repuesta A:
Con bloqueo de instalación de programas no autorizados
Quitando los permisos de administrador al sistema operativo.
Instalando el antivirus.

Repuesta B:
Se bloquea el acceso a memorias
Los usuarios no pueden instalar aplicaciones por ser usuarios sin permisos
Se protege de problemas eléctrico con UPS
Un antivirus actualizado

8. ¿Cuáles son las medidas de protección a nivel físico con la que cuentan los dispositivos de usuario final?

Repuesta A:
Protegido con UPS.
Se brinda un cable de seguridad a los usuarios de equipos portátiles.
Mantenimiento preventivo
Guardias de seguridad y cámaras de vigilancia

Repuesta B:
En las sucursales se instalan UPS y en las oficinas centrales hay generador eléctrico.
Ubicación donde las amenazas ambientales y físicas sean mínimas.
Se asigna responsables para los equipos, por medio de una hoja entrega.

9. ¿Cuál es el procedimiento para desechar los dispositivos de usuario final de forma segura?

Repuesta A:
Hay procedimiento, detallada en nuestra *Política de administración física y lógica de dispositivos* en el # 4.19

Repuesta B:
Se verifica que no tenga valor en libros con Contabilidad, pasa a la bodega y luego se desechan, para esto se levanta un acta del descarte, junto con el responsable de activo fijo de contabilidad, se retiran los discos duros, si es para desecho y si es venta o donación se formatean.

Cuestionario de evaluación C4

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.		
Entrevistado A:	Álvaro Zeledón	**Cargo:**	Gerente de TI
Entrevistado B:	Ángel López	**Cargo:**	Ingeniero de soporte senior

1. **¿Los accesos otorgados a cada usuario en los diferentes aplicativos son de acuerdo con el rol y la función definidos para la unidad de negocio correspondiente?**

Repuesta A:
Si hay diferentes perfiles o roles de acuerdo con las funciones que desempeñen.

Repuesta B:
Si, esto va en dependencia de la segregación de funciones asignadas a cada usuario.

2. **¿Se alinea la asignación de roles, funciones y responsabilidades definidas en los sistemas, basándose en los principios de menor privilegio?**

Repuesta A:
Si

Repuesta B:
Se alinea, siempre que se define cada módulo capaz de acceder solo a la información y recursos necesario para su legítimo propósito, limitando a la menor cantidad de privilegios para desarrollar acciones.

3. **¿Se identifica de manera única todas las actividades de procesamiento de información por roles?**

Repuesta A:
Si, se identifican las funciones para dar de altas los roles.

Repuesta B:
Si, previamente se recaba la información requerida para cada rol.

4. **¿Coordinan los roles con las unidades del negocio y aseguran que todos los roles están definidos consistentemente, incluyendo los roles definidos por el propio negocio?**

Repuesta A:
Si, cada unidad expone sus necesidades de y luego se revisan

Repuesta B:

Si, se involucrando a todas las unidades de negocios al generar los perfiles para cada rol en dependencia de las necesidades.

5. **Basándose en su clasificación de seguridad ¿Se autentica todo acceso a los activos de información y asegurando que los controles de autenticación han sido administrados adecuadamente?**

Repuesta A:
Si, dependiendo del rol que tenga el usuario.
Los controles de autenticación se aseguran en la fase de control de calidad de aplicaciones se realizan muchos escenarios para que la aplicación salga a producción.

Repuesta B:
Si, cada acceso tiene permisos limitados de acciones.
Se generan niveles de seguridad a partir de la administración de la base de datos, además de activar los logs y triggers y bitácoras donde se reflejen los cambios.

6. **¿Cómo se manejan las altas, bajas y cambios de accesos en los sistemas de información?**

Repuesta A:
Solicitudes por correo con formulario y autorización respectiva.

Repuesta B:
Solicitudes escritas con su respectivo formato y autorización del jefe de área.

7. **Esta gestión de acceso ¿Son las transacciones aprobadas, documentadas y autorizadas?**

Repuesta A:
Si
Repuesta B:
Si

8. **¿Cómo se gestionan y separan los niveles de acceso privilegiado?**

Repuesta A:
Para dar de alta los usuarios administradores o con permisos privilegiados se debe justificar la solicitud, también tiene que ser autorizada por *owner user* (usuario propietario) de la aplicación.

Repuesta B:
Se analiza cada caso y si en realidad se necesita para el cumplimiento de las funciones, sé gestiona.

9. **¿Realizan revisiones periódicas de la gestión de todas las cuentas y niveles de privilegios relacionados?**

Repuesta A:
Si

Repuesta B:
Si, se generan reportes de usuarios y el usuario propietario es quien debe llevar el control de las cuentas de usuario con privilegio.

10. **¿Cómo se da seguimiento al acceso de los usuarios (internos, externos y temporales) y sus actividades en los sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente?**

Repuesta A:
Si cada usuario tiene su *login* y los sistemas permiten ver quien realiza algún cambio.

Repuesta B:
Siempre que se guarde las diferentes acciones con el usuario asignado se puede tener el control de todos los movimientos.

11. **¿Se generan y conservan pistas de auditoría de todos los accesos a la información clasificada como altamente sensible?**

Repuesta A:
SI., físicas y electrónicas.

Repuesta B:
Si, en las bitácoras y tablas queda el registro del usuario en donde se observa fecha, hora y usuario que realiza el cambio.

Cuestionario de evaluación C5

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.05 Gestionar el acceso físico a los activos de TI.		
Entrevistado A:	Álvaro Zeledón	**Cargo:**	Gerente de TI
Entrevistado B:	Christian Molina	**Cargo:**	Supervisor Soporte Técnico
Entrevistado C:	Francis López	**Cargo:**	Responsable de proyectos

1. **¿Cuál es el procedimiento utilizado para las peticiones y concesiones de acceso a las instalaciones de procesamiento de datos?**

   Repuesta A:
   Está documentado la "*Política de administración física y lógica de dispositivos y aplicaciones bajo la custodia de las gerencias de IT de países*" **Numeral 6**.

   Repuesta B:
   Deberá existir una solicitud escrita del jefe o superior inmediato del tipo de acceso que solicitan ya sea física o lógica indicando el tipo de trabajo o función a realizar.
   En el caso del acceso físico se anotará en bitácora de ingreso y acompañamiento del personal de TI.

2. **¿Los perfiles de acceso a las ubicaciones de TI están definidos, actualizados y basado de acuerdo con las funciones de trabajo y responsabilidades??**

   Repuesta A:
   Si

   Repuesta B:
   En el país solo tenemos operadores de Data Center (Solo personal de TI) y gerente de país, el resto serán visitas de terceros supervisadas.

3. **¿Se registra y supervisa todos los puntos de entrada a las ubicaciones de TI, incluyendo contratistas y vendedores?**

   Repuesta A:
   Si

   Repuesta B:
   Todos los accesos son supervisados y acompañados por personal de TI.
   El centro de datos cuenta con registros fotográficos del personal que acceda.

4. **¿De qué manera se instruye al personal para mantener siempre visible su carnet de identificación?**

   Repuesta A:
   Existe un código de vestimenta y también un reglamento interno que indica portar el carnet siempre visible.

   Repuesta B:
   Por comunicación interna y revisión de cada supervisor por área

5. **¿Cómo se previene la expedición de tarjetas o placas de identidad?**

   Repuesta A:
   RRHH se encarga de tramitar el carnet de identidad y los accesos electrónicos al área que administra esta actividad (administrativa)

   Repuesta B:
   Una sola instancia (gerencia de proyectos) tiene dicha responsabilidad de emitir y entregar según el puesto.
   Repuesta C:
   RRHH o los jefes de área me solicitan el "*pase*" y yo brindo los permisos para la puerta principal y para el área que me solicitan.

6. **¿Se escolta a los visitantes en todo momento durante cualquier actividad que esté llevando a cabo en las ubicaciones de TI?**

   Repuesta A:
   Si

   Repuesta B:
   Efectivamente toda visita es escoltada por personal de TI para evitar accidentes o errores de las visitas

7. **¿Cuáles son las restricciones en el perímetro (como vallas, muros y dispositivos de seguridad) para el acceso a ubicaciones de TI sensibles?**

   Repuesta A:
   Paredes de gypsum doble tanto desde interior y exterior (4 láminas)
   Puerta de vidrio templado y oscuro
   Acceso mediante tarjetas electrónicas
   Dispositivo de vigilancia y monitoreo ambiental

   Repuesta B:
   Puertas con pases de accesos las que cuenta solo personal TI en ubicaciones sensibles

8. **¿Los dispositivos registran y envían alertas en caso de accesos no autorizados?**

   Repuesta A:
   Si, un NetBotz
   Repuesta B:
   Al no tener acceso a las puertas no existen ingresos no autorizado

9. **¿Realizan actividades regulares de capacitación en sensibilización sobre seguridad física?**

Repuesta A:
Si, existe un comité de seguridad de la información donde se abordan estos temas.

Repuesta B:
Todo empleados nuevo recibe charla de concientización de la seguridad y Capital Humano envía trimestralmente notificaciones de recordatorio.

Cuestionario de evaluación C6

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.06 Gestionar documentos sensibles y dispositivos de salida.		
Entrevistado A:	Álvaro Zeledón	**Cargo:**	Gerente de TI
Entrevistado B:	Christian Molina	**Cargo:**	Supervisor Soporte Técnico

1. **¿Cuál es el procedimiento para controlar la recepción, uso, retiro y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa?**

Repuesta A:
Para el caso de TI esto es abordado en el manual de políticas "*Guía de administración física y lógica de aplicaciones y dispositivos bajo la custodia de TI*" **#4.19 Desecho de Equipos**.

Repuesta B:
Está estipulado en la política de seguridad de la información una norma que regula y maneja estos formularios y dispositivos dentro y fuera de la empresa lo cual queda a criterio del usuario si se cumple o no.

2. **¿Se asignan privilegios de acceso a documentos confidenciales y dispositivos de salida, equilibrando riesgo y requerimientos de negocio?**

Repuesta A:
En el caso particular de nuestra compañía cada área es dueña de su propia información y el acceso a la misma ya sea de forma física o lógica se administra bajo una matriz de *Key User* u *Owner Users* quienes autorizan o deniegan los accesos de acuerdo con cada rol.

Repuesta B:
Si, en algunos casos, por ejemplo:

- Hay carpetas en servidores donde solo se asigna permiso de acceso (sea de lectura y escritura), según los soliciten los jefes de áreas.
- También en Share Point, cada usuario es responsable de compartir la información con quien estime conveniente.
- Las impresoras se les asigna a un PIN para los usuarios que imprimen documentos “confidenciales”.

3. **¿Cuenta con un inventario de documentos sensibles y dispositivos de salida, que sea conciliado periódicamente?**

   Repuesta A:
   Lo que compete a IT, llevamos control del inventario de activos tecnológicos (Hardware, licencias de software) y este es conciliado con el área contable.

   Repuesta B:
   El área de IT no cuenta con dicho inventario, seria consultar por las distintas áreas si ellos cuentan con un inventario de su documentación sensible.

4. **¿Qué medidas de seguridad físicas aplican sobre los documentos especiales y los dispositivos sensibles?**

   Repuesta A:
   Los dispositivos sensibles están ubicados en el centro de datos cuyo acceso está limitado a personal debidamente autorizado el cual ingresa al centro mediante control de acceso electrónico. Los Medios de respaldo se manejan en la caja de seguridad y en Bóveda de Banco.

   Repuesta B:
   Hay una política de seguridad aplicada sobre los dispositivos sensibles, restringiendo el acceso de estos según su área y cargo.

5. **¿Cómo se aseguran de destruir la información sensible (impresa o medios electrónicos) y proteger los dispositivos de salida?**
   (Por ejemplo, des magnetización de medios electrónicos, destrucción física de dispositivos de memoria, trituradora)

   Repuesta A:
   Algunas áreas cuentan con trituradoras de papel y digital lo que se hace es formatear la unidad de almacenamiento.

   Repuesta B:
   En las normas y políticas de seguridad hay un artículo donde se indica la destrucción de la información sensible y protección de los dispositivos de salida, los cuales están en resguardo del área de IT

Cuestionario de evaluación C7

Proceso:	DSS05 Gestionar Servicios de Seguridad		
Práctica:	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.		
Entrevistado A:	Álvaro Zeledón	**Cargo:**	Gerente de TI
Entrevistado B:	Christian Molina	**Cargo:**	Supervisor Soporte Técnico

1. **¿Cómo registran los eventos relacionados con la seguridad que se reportan por las herramientas de monitorización de seguridad de la infraestructura?**

Repuesta A:
Por medio de las alertas emitidas por los dispositivos de monitoreo y en la gran mayoría son enviadas vía correo. También en las oficinas corporativa existe en centro de monitoreo de infraestructura de TI.
Respuesta B:
Se registran a través de reportes digitalizados los cuales se envían vía correo

2. **De estos registros de Eventos ¿Identifican la información que debe guardarse por un periodo de tiempo apropiado en base a la consideración de riegos?**

Repuesta A:
Si en los correos

Respuesta B:
Todo queda almacenado en el correo.

3. **¿Cómo se define y comunica la naturaleza y las características de los incidentes potenciales relacionado con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos, para permitir una repuesta apropiada?**

Repuesta A:
Existe un procedimiento para el tratamiento de incidentes de seguridad de la información.
Respuesta B:
Por correo y por tique se reportan los incidentes, existe un nivel de escalamiento, IT Local, Service Desk corporativo, si el incidente es interno y si no se reporta al respectivo proveedor, y a este nos asigna un tique.

4. **¿Revisan regularmente los registros de eventos para detectar incidentes potenciales?**

Repuesta A:
Si
Repuesta B:
Si se revisan localmente y existen otros que son monitoreados desde nuestro corporativo.

5. ¿Cuentan con un procedimiento para la recopilación de evidencia en línea de acuerdo con las reglas locales de evidencia forense y aseguran de que todo el personal esté al tanto de los requisitos?

Repuesta A:
No
Repuesta B:
No

6. ¿Los tiques de incidentes de seguridad se crean de manera oportuna cuando la monitorización identifica posibles incidentes de seguridad?

Repuesta A:
Si, también esta detallado en el procedimiento (*Tratamiento de incidentes de la información*), la generación del tique de manera inmediata.
Repuesta B:
Si

Anexo 3. Muestra de algunas verificaciones en sitio.

(Ver evidencia completa en la Plantilla DSS05 o en la carpeta Evidencias en el CD)

Figura 1 anexo. Verificación del antivirus actualizado

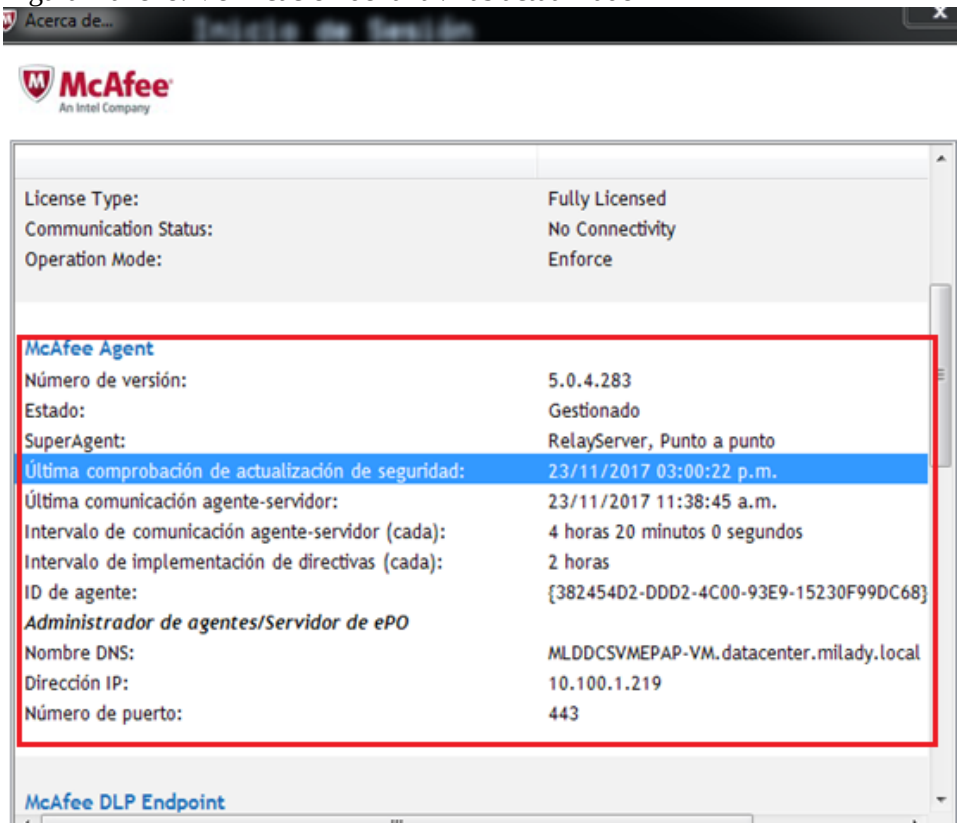


Figura 2 anexo. Verificación del antivirus actualizado, otro equipo de muestra

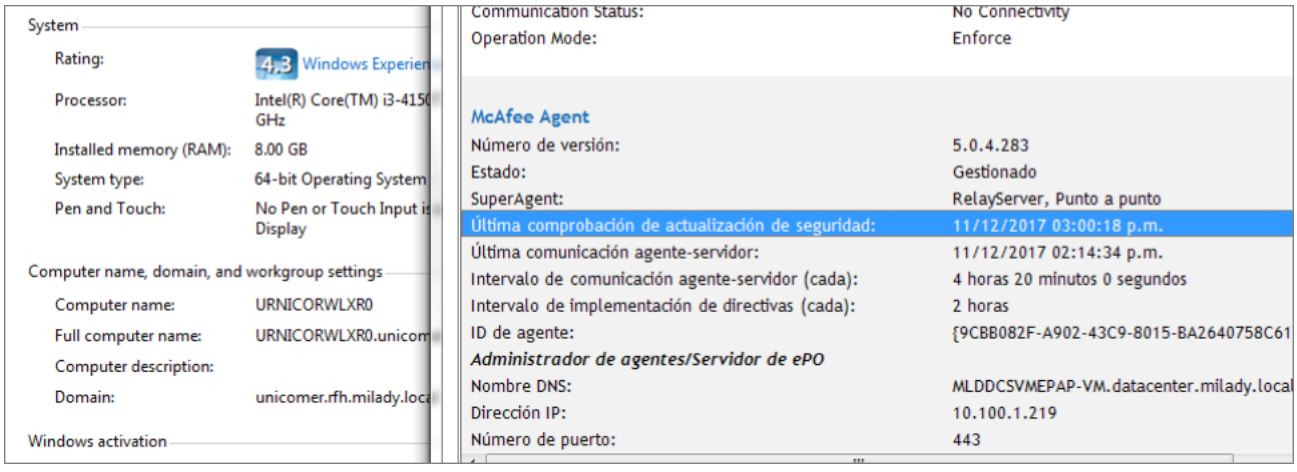


Figura 3 anexo. Verificación de Firewall

Figura 4 anexo. Verificación de filtrado de contenido de internet mediante proxy.

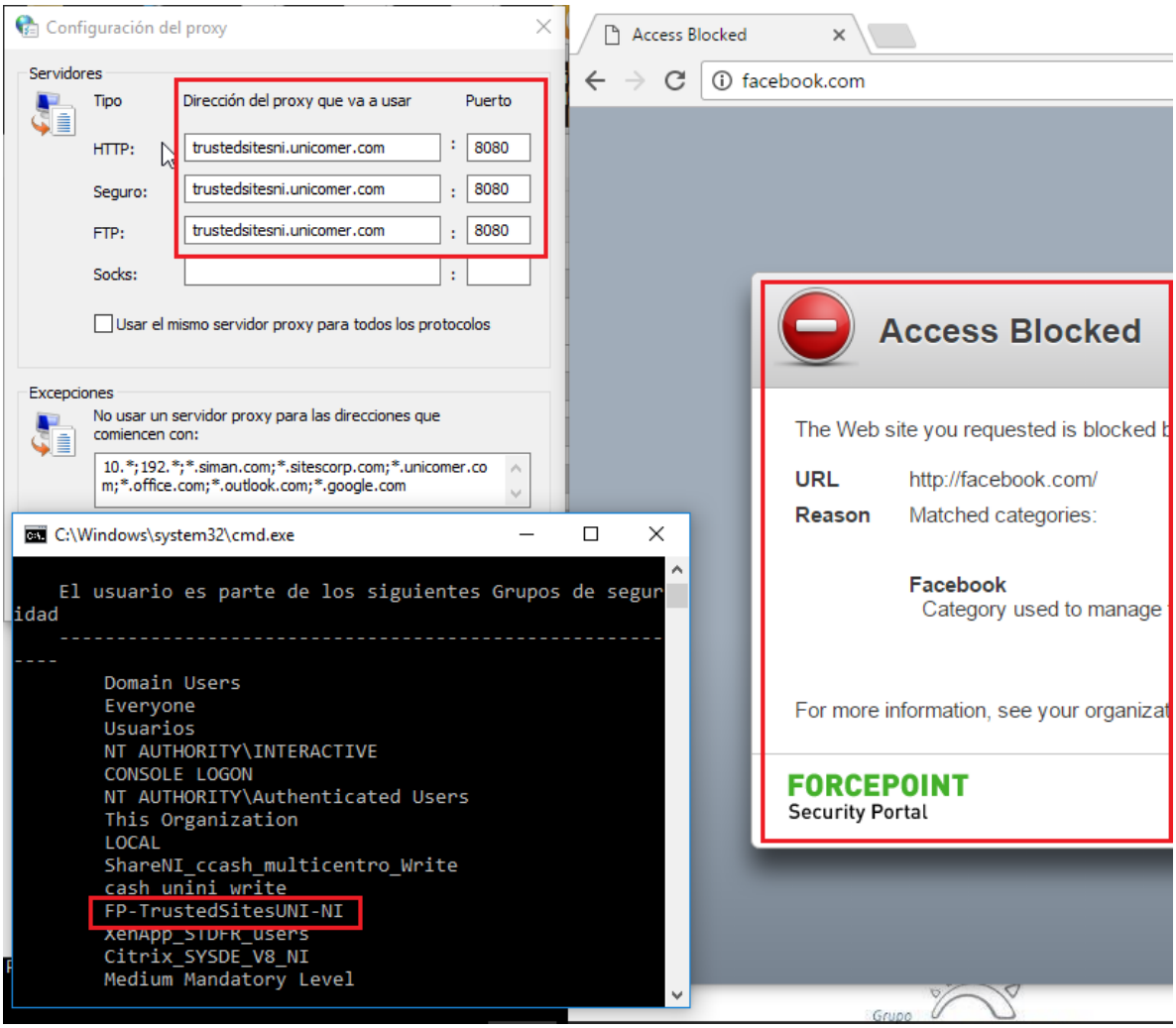


Figura 5 anexo. Verificación de que los usuarios no tienen permisos de administración

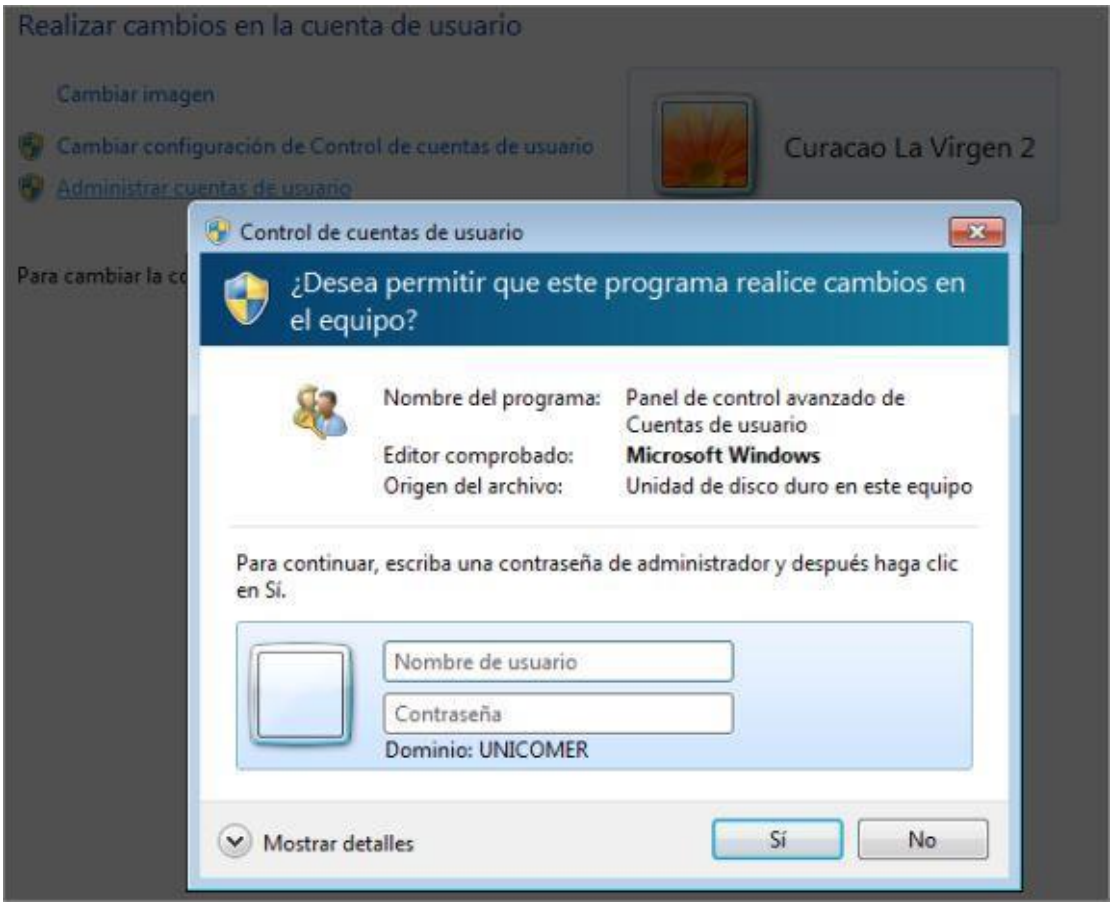
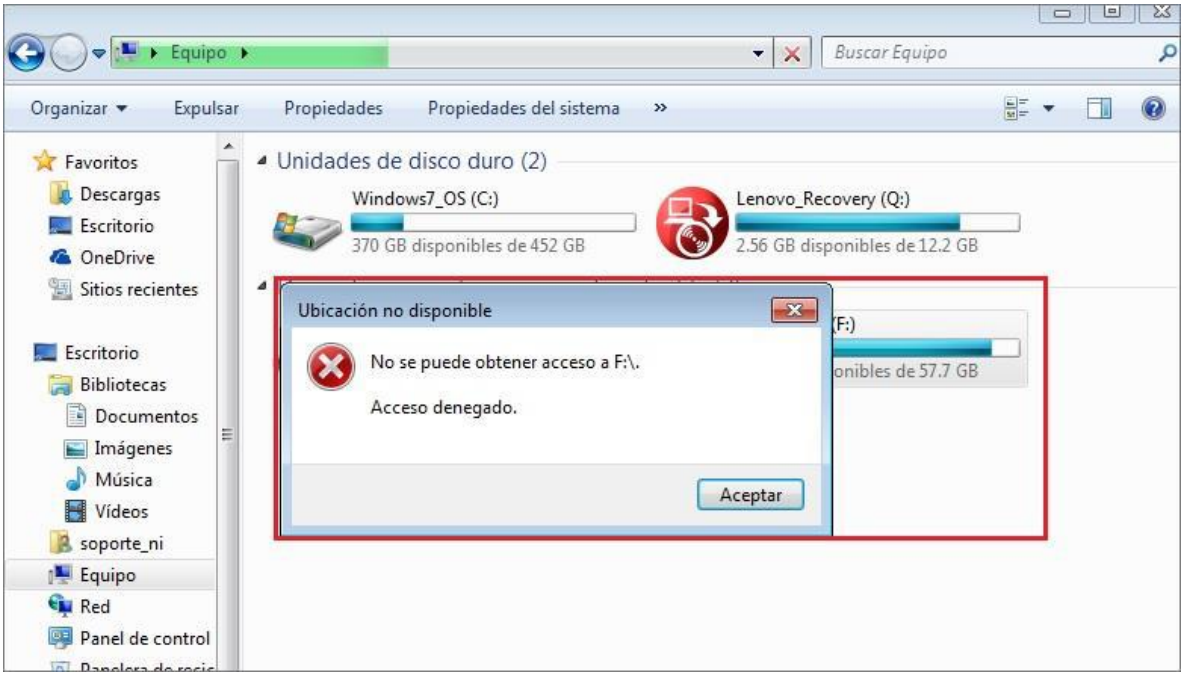
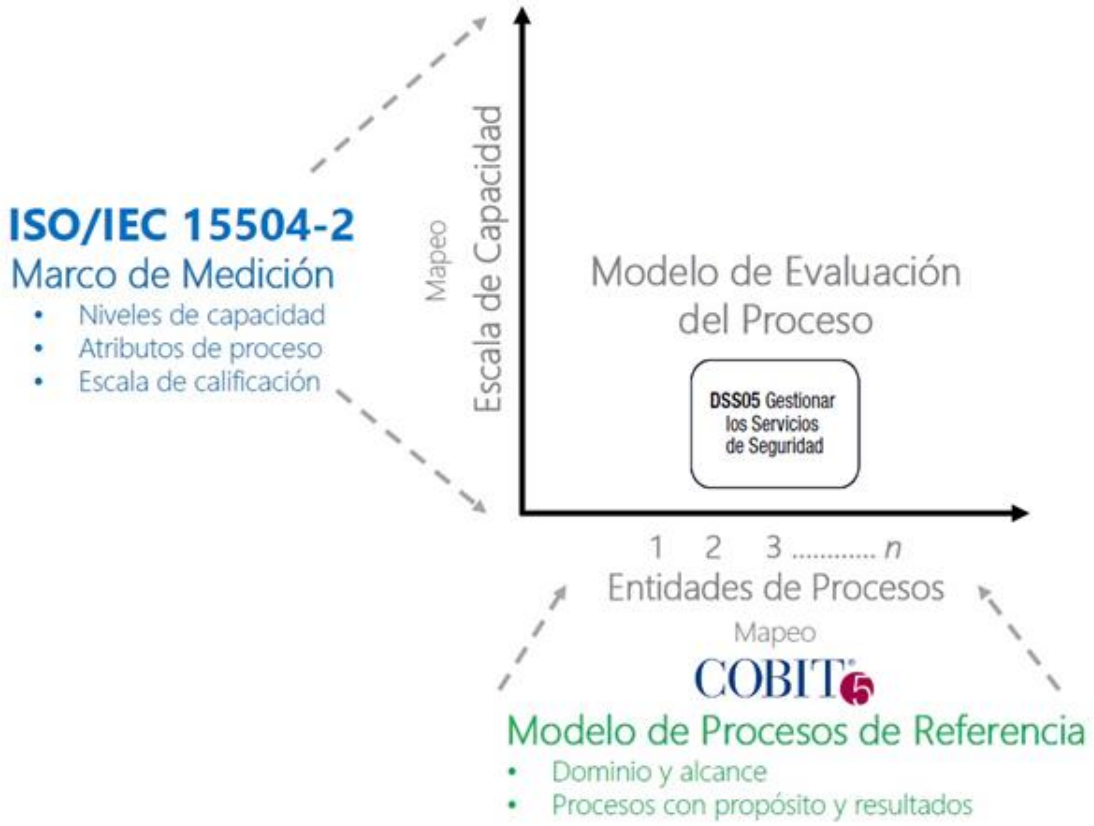


Figura 6 anexo. Verificación de bloqueo de memorias USB



Anexo 4. Modelo de evaluación ocupado para el diagnóstico.

Figura 7 anexo. Representación del modelo de evaluación ocupado para el diagnóstico.



Anexo 5. Indicadores para evaluar los niveles de capacidad

DSS05	Administrar servicios de seguridad							
	Proposito	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.						
Niveles	**Atributos Genéricos de capacidad de procesos**	**Evaluar si se logran los siguientes resultados.**	**se cumplen S/N**	**Comentario**	**No Conseguido (0-15%)**	**Parcialmente Conseguido (>15% -50%)**	**Ampliamente Conseguido (>50% - 85%)**	**Totalmente Conseguido (>85-100%)**
Nivel 0 Incompleto	**El proceso no se implementa o no logra su objetivo de proceso.**	En este nivel, hay poca o ninguna evidencia de algún logro del propósito del proceso.						
Nivel 1 Realizado o Ejecutado	**PA 1.1 El proceso implementado logra su propósito de proceso.**	**Se están logrando los siguientes resultados del proceso:**	**Calificación general para el proceso**					
		DSS05.01 Proteger contra software malicioso (malware).						
		DSS05.02 Gestionar la seguridad de la red y las conexiones.						
		DSS05.03 Gestionar la seguridad de los puestos de usuario final.						
		DSS05.04 Gestionar la identidad del usuario y el acceso lógico.						
		DSS05.05 Gestionar el acceso físico a los activos de TI.						
		DSS05.06 Gestionar documentos sensibles y dispositivos de salida.						
		DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.						
Nivel 2 Gestionado	**PA 2.1 Gestión del rendimiento del proceso:** una medida del grado al cual el funcionamiento del proceso es manejado.	Como resultado del logro completo de este atributo: a) Se identifican los objetivos para la realización del proceso. b) La ejecución del proceso se planifica y supervisa. c) La ejecución del proceso se ajusta para cumplir los planes. d) Las responsabilidades y autoridades para realizar el proceso se definen, asignan y comunican. e) Se identifican, ponen a disposición, asignan y utilizan los recursos e información necesarios para realizar el proceso. f) Las interfaces entre las partes involucradas se gestionan para garantizar tanto la comunicación efectiva como la asignación clara de responsabilidades.						
	PA 2.2 Gestión de resultado de trabajo: una medida de la medida en que los productos de trabajo producidos por el proceso se gestionan adecuadamente. Los productos de trabajo (o salidas del proceso) están definidos y controlados.	Como resultado del logro completo de este atributo: a) Se definen los requisitos para los productos de trabajo del proceso. b) Se definen los requisitos para la documentación y control de los productos de trabajo. c) Los productos de trabajo están apropiadamente identificados, documentados y controlados. d) Los productos de trabajo se revisan de acuerdo con los arreglos planificados y se ajustan según sea necesario para cumplir con los requisitos.						
Nivel 3 Establecido	**PA 3.1 Definición de Proceso:** Una medida del grado al cual un proceso estándar es mantenido para apoyar el despliegue del proceso definido.	Como resultado del logro completo de este atributo: a) Se define un proceso estándar, que incluye pautas de adaptación adecuadas, que describe los elementos fundamentales que deben incorporarse en un proceso definido. b) Se determina la secuencia e interacción del proceso estándar con otros procesos. c) Las competencias requeridas y los roles para realizar un proceso se identifican como parte del proceso estándar. d) La infraestructura requerida y el entorno de trabajo para realizar un proceso se identifican como parte del proceso estándar. e) Se determinan los métodos adecuados para controlar la efectividad y la idoneidad del proceso.						
	PA 3.2 Despliegue de Proceso : Una medida del grado al cual el proceso estándar con eficacia es desplegado como un proceso definido para alcanzar sus resultados de proceso.	Como resultado del logro completo de este atributo: a) Se despliega un proceso definido basado en un proceso estándar seleccionado y / o adaptado apropiadamente. b) Se asignan y comunican los roles, responsabilidades y autoridades requeridas para realizar el proceso definido. c) El personal que realiza el proceso definido es competente sobre la base de educación, capacitación y experiencia apropiadas. d) Los recursos necesarios y la información necesaria para realizar el proceso definido están disponibles, asignados y utilizados. e) La infraestructura requerida y el entorno de trabajo para realizar el proceso definido están disponibles, gestionados y mantenidos. f) Se recopilan y analizan datos apropiados como base para comprender el comportamiento de, y para demostrar la idoneidad y efectividad del proceso, y para evaluar dónde se puede hacer una mejora continua del proceso.						
Nivel 4 Predecible	**PA 4.1 Medida de Proceso :** Una medida del grado al cual los resultados de medida son usados para asegurar que el funcionamiento del proceso apoya el logro de objetivos de funcionamiento de proceso relevantes en apoyo de objetivos definidos de negocio.	Como resultado del logro completo de este atributo: a) Se establecen las necesidades de información de proceso en apoyo de los objetivos empresariales definidos. b) Los objetivos de medición del proceso se derivan de las necesidades de información del proceso. c) Se establecen objetivos cuantitativos para el rendimiento del proceso en apoyo de los objetivos comerciales relevantes. d) Las medidas y la frecuencia de medición se identifican y definen de acuerdo con los objetivos de medición del proceso y los objetivos cuantitativos para el rendimiento del proceso. e) Los resultados de la medición se recopilan, analizan e informan para controlar en qué medida se cumplen los objetivos cuantitativos para el rendimiento del proceso. f) Los resultados de medición se utilizan para caracterizar el rendimiento del proceso.						

Anexo 5. Indicadores para evaluar los niveles de capacidad(cont.)

	PA 4.2 Control de procedimiento: Una medida del grado al cual el proceso cuantitativamente es manejado para producir un proceso que es estable, capaz y fiable dentro de límites definidos.	Como resultado del logro completo de este atributo: a) Las técnicas de análisis y control se determinan y aplican cuando corresponda. b) Los límites de control de variación se establecen para el funcionamiento normal del proceso. c) Los datos de medición se analizan para causas especiales de variación. d) Se toman acciones correctivas para abordar causas especiales de variación. e) Se restablecen los límites de control (según sea necesario) después de la acción correctiva.						
Nivel 5 Optimizado	**PA 5.1 Innovación de Proceso:** Una medida del grado al cual los cambios al proceso son identificados del análisis de las causas comunes de variación en el funcionamiento, y de las investigaciones de accesos innovadores a la definición y el despliegue del proceso.	Como resultado del logro completo de este atributo: a) Se definen los objetivos de mejora de proceso para el proceso que respaldan los objetivos comerciales relevantes. b) Se analizan los datos apropiados para identificar las causas comunes de las variaciones en el rendimiento del proceso. c) Se analizan los datos apropiados para identificar oportunidades de mejores prácticas e innovación. d) Se identifican las oportunidades de mejora derivadas de las nuevas tecnologías y los conceptos de proceso. e) Se establece una estrategia de implementación para lograr los objetivos de mejora del proceso.						
	PA 5.2 optimización de Proceso: Una medida del grado al cual los cambios a la definición, la dirección y el funcionamiento del proceso causan el impacto eficaz que alcanza los objetivos de mejora de proceso relevantes.	Como resultado del logro completo de este atributo: a) El impacto de todos los cambios propuestos se evalúa en relación con los objetivos del proceso definido y el proceso estándar. b) La implementación de todos los cambios acordados se gestiona para garantizar que se comprenda y se actúe sobre cualquier interrupción en el rendimiento del proceso. c) Con base en el desempeño real, la efectividad del cambio del proceso se evalúa en función de los requisitos definidos del producto y los objetivos del proceso para determinar si los resultados se deben a causas comunes o especiales.						

N- 0%-15% | **P-** >15%-50% | **L-** >50%-85% | **F-** >85%-100%

N – No conseguido
P – Parcialmente conseguido
L – Ampliamente conseguido
F – Totalmente conseguido

Fuente:
https://www.isaca.org/COBIT/Documents/PAM-Using-COBIT-5-ToolKit_tkt_eng_0114.zip
Tool Kit (Requires lite registration)